



The Global Privacy and Information Security Landscape

Frequently Asked Questions



Preface

As the world becomes increasingly connected, it is critical to view information security and privacy not merely as IT issues, but also as essential business priorities. Security threats, vulnerabilities and privacy exposures challenge every organization today, creating risks that must be controlled and managed. Often organizations do not know what risks they face or how they will manage these risks. If managed properly, recognized leadership in handling personally identifiable information and driving personalized service can be a differentiator to consumers and partners and become a driver of business growth.

With this in mind, Pillsbury Winthrop Shaw Pittman LLP and Protiviti Inc. have pooled their areas of expertise to co-author *The Global Privacy and Information Security Landscape: Frequently Asked Questions*. Pillsbury provides legal overviews and insight regarding current laws and regulations, and Protiviti offers guidance to implement and maintain an effective privacy and information security program from an operational perspective.

Information security and privacy are global concerns, and thus there are many laws and regulations in countries around the world designed to protect or limit the rights of individuals and businesses. This FAQ guide discusses key laws and regulations, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the European Union General DP Directive and the Electronic Communications Privacy Act. Among the many topics addressed are privacy trends, security breaches, privacy programs, international laws and guidance for victims of identity theft. Note that the topics discussed in the first seven sections of this guide are based primarily on U.S. requirements and industry standards, although many of the principles and leading practices considered therein may be applicable internationally as well.

This guide is provided for general information only; it is not intended to give legal analysis or advice. If legal guidance is desired, companies should consult legal counsel or other appropriate advisers who can best address specific questions as they relate to their unique circumstances.

Given that the risk landscape is dynamic, and information and privacy concerns are likely to undergo significant changes in the coming years, many of the responses in this guide will evolve accordingly. As organizations strive to manage these risks, we hope this FAQ guide will prove to be a valuable resource.

Pillsbury Winthrop Shaw Pittman LLP

Protiviti Inc.

April 2010

Table of Contents

Preface	i
Background.....	1
1. Why are data privacy and protection so important?	1
2. Individuals have long been concerned about protecting their privacy, so what is driving the increased focus on privacy today?	2
3. What types of information are people most concerned about?	2
4. What is identity theft?	2
5. Why might a perpetrator steal or target health-related information?	2
6. What are some of the most common online security risks that individuals face?	3
7. What is hacking?	4
8. What is phishing?	4
9. What is pharming?	4
10. What is keystroke logging?	5
11. What is advance fee fraud?	5
12. How many people are affected by security breaches?	5
13. Is it only electronic information that is subject to risk?	5
14. What are some common, non-electronic security risks?	5
15. Beyond the misuse of personal information, are there other data usage and protection risks that should be considered?	6
16. What types of businesses have the most significant exposure to privacy risk?	6
17. What steps have lawmakers and regulators taken to address concerns about privacy?	6
18. What are the primary objectives of privacy legislation?	7
19. Why don't privacy laws protect businesses?	7
Discussion of U.S. Federal Privacy Laws and Regulations.....	8
Gramm-Leach-Bliley Act (GLBA)	8
20. What businesses are covered by the Gramm-Leach-Bliley Act (GLBA)?	8
21. Does the GLBA have different requirements for different types of customers?	8
22. What personal information is protected?	8
23. What is the difference between a “consumer” and a “customer”?	9
24. Does the GLBA mandate a privacy policy notice?	9
25. What must a privacy policy notice include?	9
26. When does a financial institution need to provide a copy of a privacy policy?	10
27. What is an “opt-out” notice and when must a financial institution provide it?	10
28. With whom may a financial institution share personal information without providing an opt-out?	11
29. Are there regulations governing the GLBA?	11
30. May a financial institution share personal information with its vendors?	11
31. Does the GLBA impose other requirements?	11
32. What are the penalties for violating the GLBA?	12

Health Insurance Portability and Accountability Act (HIPAA)12

33. What is HIPAA?12
34. How did HITECH change HIPAA?12
35. Are there regulations that govern HIPAA?12
36. Who has to comply with the HIPAA Privacy Rule?12
37. What does a HIPAA privacy policy include?13
38. When do covered entities need to provide a copy of a privacy policy?14
39. With whom may covered entities share protected health information?15
40. Do covered entities need to get consent to share protected health information with data processing vendors? . . .16
41. What document retention obligations are imposed by HIPAA?16
42. What requirements apply when there is a breach of protected health information?17

Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA) . .18

43. What is the Fair Credit Reporting Act?18
44. To whom does the FCRA apply?19
45. What is a “consumer reporting agency”?19
46. What constitutes consumer report information?19
47. Are there any instances where the exclusions for consumer report information do not apply?19
48. Who may request a consumer report?20
49. What constitutes a “business purpose” for requesting a consumer report?21
50. What is a security freeze?21
51. When is a security freeze permitted?21
52. Can a charge be imposed for freezing or unfreezing a consumer report?21
53. What is an investigative consumer report?22
54. Who may request an investigative consumer report?22
55. FCRA provides certain rights when adverse action is taken based on consumer report information.
What is an “adverse action”?22
56. When do users of consumer reports have to give notice of an adverse action?22
57. What are the Identity Theft Red Flags Rules?23
58. Who needs to comply with the Identity Theft Red Flags Rules?23
59. What is considered a “financial institution”?23
60. Who is considered a “creditor”?24
61. What type of accounts trigger compliance with the Red Flags Rules?24
62. Are the Red Flags Rules limited to consumer accounts?25
63. What business accounts are covered?25
64. Do the Red Flags Rules only cover the opening of accounts?25
65. What is meant by “multiple payments”? Do two installments qualify?25
66. Does the Identity Theft Red Flags Rules Plan have to be written?25
67. What does the plan have to include?25
68. Can policies and procedures prepared for compliance with other regulations substitute for the plan?26
69. We have a Customer Identification Program. Can that be a substitute for the Red Flags Rules Plan?26
70. We are Payment Card Industry Data Security Standard-compliant. Is that sufficient?26
71. Does the plan have to include a list of all the “red flags” we identify?26
72. Does the plan have to include all the “red flags” in Appendix J of the Red Flags Rules?27
73. How do we determine whether a circumstance is a “red flag” for identity theft?27
74. What is the deadline for compliance?27
75. What are the board of directors’ obligations under the Red Flags Rules?27

76.	How often must the plan be updated?	27
77.	What vendor oversight is required?	27
78.	Do we need to police our vendors?	28
79.	Must our vendors adopt our plan?	28
80.	What due diligence is required when we engage a vendor?	28
81.	Do we need to review all vendor contracts before the June 1, 2010 compliance deadline?	28
82.	What is the penalty for noncompliance with the Red Flags Rules?	28
83.	What enforcement mechanisms are in place under the Red Flags Rules?	28
84.	What is the penalty for violating the FCRA?	28
85.	What document retention and disposal obligations are imposed by FCRA?	29
86.	How do users dispose of consumer report information?	29
87.	If a company is not a consumer reporting agency, does the FCRA still apply?	29
88.	What are consumer reporting agencies' obligations to protect or secure consumer report information?	30
89.	Are there limitations on sharing consumer report information? What is the Affiliate Marketing Rule?	30
90.	What must be included in an affiliate marketing disclosure?	30
91.	What is an "affiliate"?	31
92.	What information is considered "experiential"?	31

Children’s Online Privacy Protection Act (COPPA)31

93.	What is the Children’s Online Privacy Protection Act?	31
94.	To whom does COPPA apply?	31
95.	What information may website operators collect from a child without first obtaining parental consent?	31
96.	How do operators verify that a parent has consented?	32
97.	What security procedures must operators have in place when they hold children’s information?	32
98.	What verification should operators require for someone to access the child’s information?	32
99.	How does one determine whether a website “attracts” children?	32
100.	An operator wants to offer birthday coupons to children. Does it have to comply with COPPA?	33
101.	What do operators need to do to verify the child’s age?	33
102.	What should an operator do if it suspects children are using its site and providing information?	33
103.	Can website operators market to children over the age of 13?	33
104.	Does COPPA apply to off-line information collection?	34
105.	Do pictures of children constitute “information”?	34
106.	What are the penalties for violating the statute?	34
107.	Are there other laws or regulations that limit marketing to children?	34

Right to Financial Privacy Act (RFPA)34

108.	What is the Right to Financial Privacy Act?	34
109.	Who is covered by the RFPA?	35
110.	What is a “financial institution” for purposes of the RFPA?	35
111.	Do the protections under the RFPA extend to all of an institution’s customers, or only to individuals?	35
112.	Upon receipt of a government agency request for financial records, does an institution need to notify its customer?	35
113.	Are any records excluded from the RFPA?	35
114.	What are an institution’s reporting obligations under the RFPA?	36
115.	Are there regulations that govern or relate to the RFPA?	36
116.	Are there similar statutes at the state level?	37
117.	What is the penalty for violating the RFPA?	37

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) . . .37

118. What is CAN-SPAM? 37

119. What communications are covered by CAN-SPAM? 37

120. Does CAN-SPAM apply to business-to-business communications, as well as communications to consumers? 38

121. What are the requirements for compliant e-mails? 38

122. Does CAN-SPAM prohibit broad e-mail “blasts”? 39

123. Can senders e-mail existing customers without restriction? 39

124. Are only advertising e-mails covered by CAN-SPAM? 39

125. What are senders’ obligations to provide “opt-outs”? 39

126. A company has an e-mail newsletter service for customers. Can it add customers without their consent? 39

127. Can senders sell their customers’ e-mail addresses? 39

128. What is the penalty for violating CAN-SPAM? 40

129. Who is at risk if there is a violation? 40

130. Is there a “Do Not E-mail” registry? 40

131. Are there similar laws on the state level that one needs to be aware of? 40

Electronic Communications Privacy Act (ECPA)41

132. What is the Electronic Communications Privacy Act? 41

133. Who needs to comply with the ECPA? 41

134. Are ISPs covered? 41

135. What privacy obligations are imposed by the ECPA? 41

136. What security obligations are imposed by the ECPA? 42

137. What are the protections required for stored communications? 42

138. What are the protections required for transmitted communications? 43

139. What is the penalty for violating the ECPA? 43

Telephone Consumer Protection Act (TCPA)44

140. What is the TCPA? 44

141. What are the requirements of the TCPA? 44

142. Who must comply with the TCPA? 44

143. Who enforces the TCPA? 44

144. What kind of damages may an individual recover from a telemarketer who violates the TCPA? 44

145. What types of defenses are available to telemarketers if they violate the TCPA? 45

146. Under the TCPA, what is the daily window of time when it is impermissible for telemarketers to place telephone calls? 45

147. What disclosures are required by telemarketers as part of the TCPA? 45

148. Under the TCPA, what is a “telephone solicitation”? 45

149. What is the Do Not Call Registry? 45

150. Does the TCPA pre-empt any state laws related to telemarketing? 45

151. Are there any state-specific do-not-call laws? 45

152. What is the Junk Fax Protection Act of 2005? 46

153. What requirements must marketers comply with under the Junk Fax Protection Act of 2005? 46

154. What is the “Existing Business Relationship” exception under the Junk Fax Protection Act of 2005? 46

Discussion of U.S. State and Local Laws and Regulations 47

155. What governmental bodies have authority to enforce privacy laws and regulations?	47
156. What state laws exist related to sharing of Social Security numbers?	47
157. What is California’s “Shine the Light” statute?	47
158. What is the Massachusetts Regulation “Standards for the Protection of Personal Information of Residents of the Commonwealth”?	49
159. What is Nevada’s “Restrictions on transfer of personal information through electronic transmission”?	49
160. What is Minnesota’s “Access Devices; Security Breach” statute? [M.S.A. § 325E.64]	49
161. What are some of the standards that states use to apply their privacy laws to out-of-state businesses?	49
162. What are some of the current state-level trends in privacy law regulation?	50

Intersection of U.S. Privacy Laws with Other Laws and Regulations 51

163. Are there any circumstances where law enforcement’s interest overrides an individual’s right to privacy?	51
164. What is the USA PATRIOT Act?	51
165. What types of personal information may be released under the terms of the USA PATRIOT Act?	52
166. What information triggers filing a Suspicious Activity Report?	52
167. What is a National Security Letter?	52
168. Are there instances where privacy laws may negatively affect a company’s efforts to comply with other mandates?	53
169. Are there circumstances in which health-related information may be disclosed without the owner’s permission?	53

Privacy Trends and Standards in Other Industries 54

170. What are some of the more significant legal risks related to privacy today?	54
171. What privacy issues surround social networking?	54
172. What are the privacy implications of cloud computing?	54
173. Are there any private sector initiatives to protect privacy?	55
174. What is the Payment Card Industry Data Security Standard (PCI DSS)?	55
175. What types of companies are subject to PCI DSS?	55
176. What are the consequences of not complying with PCI standards?	55
177. What is NACHA?	55
178. How does the ACH network operate?	56
179. What privacy requirements does NACHA impose?	56
180. What are the consequences of not complying with the NACHA requirements?	58
181. What is multifactor authentication?	58
182. How have companies tried to educate their customers about privacy and information security?	58

Developing and Maintaining an Effective Privacy Program. 59

183. What are the key elements of an effective privacy program?	59
184. How do you conduct a privacy risk assessment?	59
185. What should privacy policy and procedures address?	60
186. What should an effective vendor management program include?	60
187. Who in a company should “own” the privacy policy?	61

Information Security 62

188. What is the typical relationship between a company’s privacy and information security programs?	62
189. What are the elements of an effective ISP? Does it need to be a single document?	62
190. Are there any regulations that specifically require companies to implement written ISPs?	63
191. If my company is not specifically required by regulation to implement a written ISP, is there any reason why we should consider implementing such a program?	63
192. What types of data should be addressed within an ISP? Do information security-related regulatory requirements apply only to consumer information, or also to information about a company’s business customers and employees?	63
193. Should the scope of an ISP be limited to electronic data?	64
194. In some industries (notably, banking), the ISP must be approved by a company’s board of directors. As a leading practice, what level of detail should be presented to the board for its review?	64
195. How should an information security risk assessment (ISRA) be conducted? How does the ISRA process differ from the privacy risk assessment process?	64
196. What are some of the common weaknesses and/or areas of regulatory criticism related to ISPs and/or ISRAs?	64
197. What types of information security requirements apply to Internet banking?	65
198. Is multifactor authentication truly required for all Internet-banking transactions?	65
199. Who in a company should “own” the ISP? Should the privacy and ISP owner be the same person?	65
200. How often should a company consider reviewing and updating its ISRA and ISP?	66
201. What are the key risks associated with a failure to maintain an effective ISP?	66

Addressing Security Breaches 67

202. What is a security breach?	67
203. What constitutes “personal information”?	67
204. Which definition applies in my situation?	68
205. How many states have a data breach notification law? What are some of the differences among the data breach notification laws enacted by these states?	68
206. Is there a federal law requiring notification for security breaches?	68
207. Is “computerized information” limited to a database in a computer or on a server containing personal information?	68
208. What is the difference between data that is “accessed” and data that is “acquired”?	69
209. What about data that is “lost”?	69
210. How do I discover a security breach?	69
211. What steps should I take when I first learn that there may be an intrusion into our system or a loss of data?	69
212. An employee accessed the database. Can that be a security breach?	70
213. Who should be involved in the investigation process?	70
214. When should I call law enforcement?	71
215. Who should be called?	71
216. Is there a time limit on when I have to send out the notices?	71
217. What if I don’t have sufficient contact information to send a letter?	71
218. Can I send notice by e-mail if I have an e-mail address?	71
219. Can I give notice by telephone?	72
220. What information needs to be included in the notice letter?	72
221. What is “substitute notice”?	72

222. Is notice limited to cases where the information is known to have been misused?	73
223. What protocols should be in place to make the response more efficient?	73
224. Is a call center required?	73
225. Is the response different for different types of information (e.g., Social Security numbers vs. driver’s license numbers)?	73
226. Which state or local agencies must receive notice?	74
227. I maintain or have licensed someone else’s data. Am I required to give notice?	74
228. What are the penalties for not complying with the law?	74

What Do You Do If You Are the Victim of Identity Theft? 75

229. What are the steps I should take if I am a victim of identity theft?	75
230. What is a fraud alert?	76
231. What is a credit freeze?	76
232. What is an identity theft report?	76
233. What do I do if the police only take reports about identity theft over the Internet or telephone?	77
234. What do I do if the local police won’t take a report?	77
235. How do I prove that I’m an identity theft victim?	77
236. Should I apply for a new Social Security number?	78

International Laws and Regulations 79

International Privacy Background 79

237. Approximately how many countries have data privacy and protection laws?	79
238. Other than national laws, what other organizations have a role in international privacy law and policy?	79
239. How do the various national and regional privacy authorities differ?	80
240. What challenges exist for multinational corporations that collect data in these various jurisdictions?	81

Asia-Pacific Economic Cooperation (APEC) Privacy Framework 81

241. What is the APEC Privacy Framework?	81
242. What are the nine APEC Privacy Framework principles?	82
243. What are Cross-Border Privacy Rules (CBPRs)?	82
244. Who will enforce the APEC Privacy Framework?	82
245. What challenges does APEC face in developing its Privacy Framework?	82
246. What countries will be a party to APEC?	82
247. How does the APEC Framework differ from the European Union’s approach to privacy and data security?	83

Japan 83

248. What is Japan’s Personal Information Protection Act (PIPA)?	83
249. Under PIPA, what is “personal information”?	83
250. Who must comply with PIPA?	83
251. Who enforces PIPA?	83
252. Are there other notable Japanese privacy and data security laws?	84

The Americas	84
253. What countries in South America have comprehensive privacy laws?	84
254. What is “Habeas Data”?	84
255. How are Brazil’s privacy laws organized?	84
256. What are the notable privacy laws in Argentina?	85
Canada	85
257. What is PIPEDA?	85
258. When does PIPEDA apply?	85
259. What is considered “personal information” under PIPEDA?	85
260. How does Canada’s definition of personal information in PIPEDA differ from the European Union’s definition?	86
261. What remedies are available as a result of a breach of PIPEDA?	86
262. Are there any provincial privacy laws in Canada that impose more stringent privacy standards than PIPEDA?	86
European Union Privacy and Information Security Laws and Regulations – A Closer Look	87
The European Union (EU) Data Protection Directives	87
263. What are the European Union (EU) Data Protection Directives?	87
264. What is the purpose of the EU General DP Directive?	88
265. What role do the EU member states play?	88
266. What are a DPA’s obligations?	89
267. What powers do the DPAs have?	89
268. What is the “Working Party”?	89
269. What does the General DP Directive mean to companies/organizations?	89
270. What is considered personal data under the General DP Directive?	90
271. What is a data controller?	90
272. What is a data processor?	90
273. What is the difference between a controller and processor of data?	90
274. What is a data subject?	90
275. What is an “establishment” under the Directive?	91
276. What constitutes “use of equipment” under the Directive?	91
277. When and where are data protection rules applicable?	91
278. What are the rules on the processing of personal data?	91
279. What are the rules on the collection of data?	91
280. What are the principles relating to data quality?	91
281. What are the criteria for making data processing legitimate?	92
282. What are the rules on unsolicited communications and electronic direct marketing?	92
283. What are the businesses’ obligations to retain data?	92
284. Who should have access to retained data?	92
285. What are the retention periods?	93
286. Are there any guidelines on data protection and data security in relation to retention?	93
287. Should businesses ensure confidentiality of processing?	93
288. How should businesses ensure security of processing?	93

289. What if data processing is carried out by a third party?	93
290. What is notification?	94
291. What are the contents of notification?	94
292. What are the consequences of not complying with the Directives?	94
293. What typical privacy policies should a business implement to maintain data privacy regulations?	94
294. What is cloud computing and what data privacy issues are related to it?	95
The General DP Directive and Transfer of Personal Data to Third Countries.	95
295. What does the General DP Directive mean to companies outside Europe?	95
296. What is an “adequate level of protection”?	96
297. What happens if an adequate level of protection is not in place in the third country?	96
298. What if there is conflicting opinion between the European Commission and the member state with regard to the adequate level of protection?	96
299. Are there any exceptions that allow the transfer of data to a third country that does not ensure an adequate level of protection?	97
300. What options are available to organizations when transferring personal data out of EU countries?	97
301. What are standard contractual clauses?	98
302. What are the principles behind the standard contractual clauses?	98
303. How many sets of clauses are there?	98
304. Why are there two sets of standard contractual clauses and what are the main differences between them?	99
305. Are the standard contractual clauses compulsory for companies interested in transferring data outside the European Union?	99
306. Can companies implement the standard contractual clauses in a wider contract and add specific clauses?	99
307. How are Binding Corporate Rules used?	100
308. Can U.S.-based companies that have not joined the Safe Harbor Accord use the relevant Safe Harbor rules under the contract?	101
The Safe Harbor Agreement	101
309. What is the Safe Harbor Agreement?	101
310. Are all U.S. organizations trading with EU countries required to register for Safe Harbor?	101
311. How does an organization join the Safe Harbor program?	101
312. How do EU companies find out whether a U.S. organization is Safe Harbor registered?	102
313. What are the Safe Harbor Principles and what is required?	102
314. How is eligibility for Safe Harbor determined?	102
315. How and where is the Safe Harbor program enforced?	103
316. Approximately how many U.S. organizations have filed under Safe Harbor?	103
317. What are the consequences of failing to comply with Safe Harbor requirements?	103
The U.K. and the EU Data Protection Directives.	104
318. How has the United Kingdom addressed the EU Data Protection Directives?	104
319. Which authority in the United Kingdom administers compliance with the General DP Directive?	105
320. What geographical areas are covered by the U.K. DPA?	106
321. Why should businesses comply with the DPA?	106
322. What are companies’ obligations under the DPA?	107
323. What are the implications for data controllers with paper-based records?	107
324. What are the time periods for data controllers to respond to data requests?	107
325. What are companies’ rights under the DPA?	108

326. What are companies' obligations under the Privacy and Electronic Communications Regulations 2003?	108
327. What are companies' rights under the Privacy and Electronic Communications Regulations 2003?	108
328. What are the consequences of noncompliance?	108
329. What is notification?	109
330. Why do data controllers have to notify?	109
331. What information must be included in the notification?	109
332. Are there any exemptions to notification?	110
333. How can companies find out if they are exempt?	110
334. Are there any non-exempt areas?	110
335. How can companies notify the ICO?	111
336. What are the consequences of not notifying?	111

The Netherlands (NL) and the EU Data Protection Directives 111

337. What is the “Wet bescherming persoonsgegevens” (Wbp)?	111
338. Which authority in the Netherlands is responsible for data protection pursuant to the General DP Directive?	112
339. What are the duties of the Dutch DPA?	112
340. What guarantees apply regarding a proper performance of the tasks of the DPA?	112
341. What powers does the Dutch DPA have?	112
342. What are the individual's entitlements and company's obligations for individuals under the Wbp?	113
343. When does the Wbp apply to the data processing of companies that operate internationally?	113
344. When is the transfer of personal data to third countries (within and outside the EU) permitted?	113
345. What are the penalties for data controllers if they breach the law?	114
346. What is notification?	114
347. What information needs to be notified?	114
348. Which personal data processing does not apply in the Wbp?	114
349. How can a data processor determine if it is exempt?	115
350. How can the Dutch DPA be notified?	115
351. What are the consequences of not notifying?	115

Italy and the EU Data Protection Directives 115

352. How has Italy addressed the EU Data Protection Directives?	115
353. Which authority in Italy is responsible for supervision, pursuant to the Data Protection Directives?	116
354. What powers does Garante have?	116
355. What are individuals' rights under the D.Lgs. 196/2003?	116
356. What are the implications for data controllers with paper-based records?	117
357. What are companies' obligations under the D.Lgs. 196/2003?	117
358. What are the consequences of noncompliance?	117
359. What is notification?	118
360. What information needs to be notified?	119
361. Are there any exemptions to notification?	119
362. How can I find out if I am exempt?	119
363. How can notification be performed?	119
364. What are the consequences of not notifying?	119
365. What is the Security Policy Document (Documento Programmatico sulla Sicurezza)?	119

<i>Appendix A</i>	
	U.S. Legal and Regulatory Resource Summary 121
<i>Appendix B</i>	
	A Timeline of Pertinent Laws and Regulations 123
<i>Appendix C</i>	
	United Kingdom: Case Studies of Companies Breaking the Data Protection Act 1998..... 124
<i>Appendix D</i>	
	United Kingdom: Case Studies of Companies Breaking the Privacy and Electronic Communications Regulations 124
<i>Appendix E</i>	
	Italy: Case Study on Security Measures in Processing Telephone Traffic Data 125
<i>Appendix F</i>	
	References – European Union Privacy and Information Security Laws and Regulations 125
<i>Appendix G</i>	
	Terms and Definitions and Useful Websites 127
	About Pillsbury Winthrop Shaw Pittman LLP..... 129
	About Protiviti Inc.. 130



Background

1. Why are data privacy and protection so important?

Information privacy, or data privacy, is generally defined as the relationship among the collection and dissemination of data, technology, the public's expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information is collected and stored in digital form or otherwise.

Today, more than ever, intangible assets such as customers, systems and information provide a foundation upon which corporate value is built. Increased emphasis has been placed on customer relationship management and consumer choice as a means of gaining market share, especially in industries where mature products have become commodities. Consumers want personal choice, yet they do not want to sacrifice control over their personal information. Customers want easy access to information – through the Internet and wireless technology – but want to believe that any personal information they transmit is secure and being handled in an appropriate manner to protect it from unauthorized access.

There are myriad consumer privacy and data protection requirements globally, including, for example, the European Union's Data Protection Directive, numerous member state requirements, the U.S. Safe Harbor Agreement, the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA).

Despite a growing number of laws and regulations, stories of identity theft, inadvertent release of customer data, the loss of personal information and successful attempts by hackers to penetrate websites and steal proprietary information command headlines in the media. In turn, these events serve to raise the public consciousness, often prompting demands for more protection. Ensuring the privacy of customer information and protecting critical corporate data have become front-of-mind issues for management teams. While certain industries, such as financial services, healthcare and the public sector, may draw the most scrutiny, all industries are affected by privacy regulations, which impact their business models for providing goods and services to consumers, as well as other businesses.

As a result, large and small companies alike are assessing their privacy strategies and programs in order to achieve the following:

- Compliance with regulations
- Market differentiation
- Increased sales
- Customer satisfaction
- Protection of reputation

2. Individuals have long been concerned about protecting their privacy, so what is driving the increased focus on privacy today?

Perhaps the most significant reason for the increased focus on privacy has been the rapid expansion of laws and regulations that require companies and governmental agencies to notify consumers when breaches of sensitive data occur. The first such U.S. law, California's Senate Bill (SB) 1386,¹ became effective in July 2003. Since then, at least 44 states, the District of Columbia, and Puerto Rico have enacted similar laws.² The federal banking regulatory agencies have also issued guidelines that impose substantially similar requirements. Although most studies suggest that the actual incidence of identity theft and other privacy-related threats has been increasing steadily, there is no question that public disclosure requirements imposed by laws and regulations like California's SB 1386 have brought to light breaches that might not have been disclosed at all, or would have received little attention, in the past. The combination of breach notification laws and increased mainstream media coverage has increased the awareness and sensitivity of the general population to these issues.

3. What types of information are people most concerned about?

Most of the various privacy-related laws and regulations impose their own specific definitions of what types of data elements are considered sensitive information (which may be referred to by various terms such as "nonpublic personal information" or NPI and "personally identifiable information" or PII). However, sensitive information can generally be categorized as follows:

- Sensitive personal information (e.g., date of birth, Social Security number (SSN or other government identification number), driver's license number, mother's maiden name)
- Sensitive financial information (e.g., information pertaining to a consumer's income, assets and credit history)
- Sensitive health information (e.g., information about a consumer's medical conditions or prior medical treatment)

4. What is identity theft?

Identity theft refers to all types of crimes in which someone wrongfully obtains and uses another person's personal data in a fraudulent or deceptive way, typically for economic gain.³ The most common example of identity theft is a scenario in which a person applies for credit using another person's name, SSN/government ID number and credit history, obtains the loan proceeds or the goods purchased using the loan (e.g., an automobile), and then disappears. Once such a transaction has been conducted, this type of fraud is often only detected when the loan becomes delinquent and the creditor initiates collections efforts and locates the person who turns out to have been a victim of identity theft. This sets in motion what is often a long and difficult process for the victim to dissociate him or herself from the debt in question and clear it from a credit report.

This scenario differs from account takeover fraud, where a perpetrator steals a consumer's existing credit card (or credit card number) and purchases goods or services using the card, or accesses a consumer's existing bank account and improperly transfers funds to the perpetrator or a third party.

In each of these cases, the affected individual has had someone improperly make use of his or her personal and sensitive information for illicit financial gain.

5. Why might a perpetrator steal or target health-related information?

Aside from the fact that most people consider health information to be highly sensitive in general, some of the possible risks associated with a breach of healthcare information could include:

- Identity theft – Because health records often contain other sensitive information such as date of birth and SSN/government ID number, the identity of patients can be stolen in an attempt to obtain various health (insurance) benefits, open credit card accounts, and create fake documents such as driver's licenses.

¹ Cal. Civ. Code § 1798.82

² Information provided by the National Conference of State Legislatures as of December 9, 2009: <http://www.ncsl.org/Default.aspx?TabId=13489>

³ <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>

- Blackmail – The person who commits the breach threatens to disclose sensitive medical information (e.g., a health condition) to a patient’s family, employer, or other party unless financial or other demands are met.

In addition, the loss of vital patient details related to therapy, research and/or treatment could result in the delay of treatment, or the inability to treat, certain patients with serious illnesses. It could also limit the success of a healthcare organization’s research efforts to discover additional treatments or cures for diseases.

6. What are some of the most common online security risks that individuals face?

Following is a summary of the more common online security risks:

Malware

Viruses

- A virus is a malicious computer program or programming code that infects, disrupts, or disables a file or program on a computer. Each time the infected program is run, the virus is also triggered. It spreads itself by infecting other programs on the same computer.
- Viruses can be transmitted as attachments to an e-mail or in a downloaded file, or be present on removable media (e.g., a flash drive or CD-ROM).
- Viruses typically require the user of a machine to take an overt action to infect the machine (such as opening an infected attachment). However, malware is becoming increasingly sophisticated; for instance, users can unknowingly download them simply by visiting legitimate websites that have been compromised.

Worms

- A worm is a self-replicating computer program. However, unlike a virus, it does not infect other program files on a computer. Instead, a worm runs on its own and spreads itself automatically to other computers through e-mail or other network connections like Internet Relay Chat (IRC). Worms typically consume communication resources and slow down response times.

Trojan Horse Viruses

- A Trojan horse virus is a computer program that contains malicious or harmful code hidden inside programming or data that appears to be harmless or benign.
- Trojans are often downloaded on the back of a free program (freeware) that has some value to the user (e.g., a free game, software programs or music).
- The Trojan can be programmed to open by itself and run without any user knowledge or intervention.

Spyware

- Spyware is software that is installed on a hard drive to gather information about individuals and their computer habits. It then transmits the information through an Internet connection to a third party, usually without the individual’s knowledge or consent.
- Spyware is one of the most significant Internet security risks for today’s computer users. Some estimates suggest that 80 to 90 percent of computers have been infiltrated by spyware.

Eavesdropping

- Eavesdropping occurs when a third party covertly intercepts and observes the transmission of data between computers. Two common eavesdropping techniques are “keyloggers” (which capture users’ keystrokes) and “man-in-the-middle” attacks (which literally force all communication through the attackers’ computers so all communication traffic to a particular site can be viewed).

Snooping

- Snooping is unauthorized access to another person’s or company’s data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.

- Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to monitor activity on a computer or network device remotely.

Spam

- Spam, a form of bulk mail, is unsolicited e-mail on the Internet. It is often sent to a list of users obtained from a "spambot" (a computer program that assists in sending spam) or by companies that specialize in creating e-mail distribution lists.
- Similar to worms, the impact of spam is that it consumes limited network resources with illegitimate or other unwanted activity. Further, spam messages fill e-mail inboxes and require time and attention by the user to remove.
- Some spam is also used to transmit viruses and Trojan horses.
- Some spam is used in "phishing" or "pharming" attacks or other types of fraud employed to obtain personal information from unsuspecting consumers.

Embedded Metadata

- Microsoft Office and other types of programs can contain hidden information that the user had no intention of sharing. Some versions of Microsoft Word, for example, can track any alterations and changes that have been made while writing a document. A chart embedded in a Microsoft PowerPoint document can include the entire Microsoft Excel workbook containing the chart's data. Although these can be useful functions, the privacy concern is that this information may be accessible to third parties with whom the author had no intention of sharing the data.

Web Bugs

- A web bug, also known as a "web beacon" or "tracking bug," is a file object (usually a graphic image) that is placed on a web page or in an e-mail message to monitor user behavior and functions as a kind of spyware.
- A web bug is typically invisible to the user because it is transparent (it matches the color of the page background) and takes up only a tiny amount of space.

Tracking Cookies

- A tracking cookie is a data packet used for tracking users' surfing habits. Tracking cookies are typically used by advertisers to analyze the effectiveness of advertising data, but they may be used to profile and track user activity more closely.

7. What is hacking?

Hacking refers generally to the unauthorized use of computer and network resources. The most common example of a hacking attempt is an outside party who attempts to penetrate an organization's computer network in order to access the sensitive information maintained on that network, disrupt normal processing, or deface the site.

8. What is phishing?

Phishing is a fraud method in which the perpetrator sends out an e-mail that mimics or purports to be from a legitimate source (such as a consumer's bank or the Internal Revenue Service) in an attempt to gather personal and financial information from recipients. Information gathered as a result of successful phishing attempts is often used to perpetrate other types of fraud, such as an account takeover or full-scale identity theft. Phishing is increasingly being used against a company's employees to obtain login information and passwords to gain access to a company's internal systems.

9. What is pharming?

Pharming is a practice whereby a malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent. The "pharmed" site is typically made to look exactly like the legitimate site. Pharming has been called "phishing without a lure." Similar to phishing attempts, the purpose of pharming is generally to collect information that can be used to commit identity theft and/or account takeovers.

10. What is keystroke logging?

Keystroke logging (also known as keylogging) is a method of capturing and recording user keystrokes. Keylogging can serve multiple legitimate (or at least arguably legitimate) purposes, including determining sources of errors in computer systems, studying how users interact with systems, and measuring employee productivity on certain clerical tasks. Keystroke logging may also be used inappropriately as a means of obtaining user names, passwords, encryption keys and other sensitive information in a manner that avoids other information security measures.

11. What is advance fee fraud?

Advance fee fraud occurs when one party induces the other to make a relatively small transfer of money in exchange for a larger but nearly always nonexistent future payoff. Perhaps the best known of these types of scams is the “Nigerian 419 letter”⁴ scheme. In most variations, this involves an e-mail request from a party purporting to represent a foreign government, royal family or similarly wealthy party. The e-mail sender suggests to the recipient that the sender intends to transfer a large amount of money into the recipient’s country of residence, and promises a significant percentage of the total transfer amount if the recipient will pay a “funding fee” or similar up-front charge to the sender.

12. How many people are affected by security breaches?

Estimates vary widely; however, the number is easily in the tens, if not hundreds, of millions each year in the United States alone. The Privacy Rights Clearinghouse estimates that more than 345 million records have been compromised since January 2005.⁵

13. Is it only electronic information that is subject to risk?

No. The risk to electronically stored data is highlighted perhaps because most U.S. state laws only require disclosure of compromises involving electronically stored data.⁶ Thus, external “hacking” threats are those typically raised by the general media and public in discussions about security risks. However, since 2005, U.S. financial institutions subject to banking agency supervision have been required to provide notification of information compromises involving any media where there is a risk of harm to the institution’s customers.⁷ History shows that a significant percentage of security breaches are caused by improper control and/or disposal of hard copy information, and/or human errors in transmitting or maintaining electronic information.

It is important to remember that the Internet and other tools used for digital communication are just new technologies being leveraged to perform “traditional” forms of crime. The old approaches have not disappeared; they have been supplemented (and, in many cases, made more effective) by advances in technology.

14. What are some common, non-electronic security risks?

Some of the most common, non-electronic security risks include (but are not limited to):

- Physical human error (e.g., incorrect processing, misplacement of private information).
- Theft, loss or insecure disposal of hard copy media (e.g., laptops, backup tapes, flash drives).
- Insecure storage or disposal of sensitive printed records. (Consider, for example, the large number of publicized breaches brought to light as a result of “dumpster diving” experiments that found customer loan files, credit card statements, medical records and similar information having been thrown away rather than shredded.)
- Insufficient physical or administrative security measures to restrict access to areas where sensitive information is stored.

⁴ “419” refers to the section of the Nigerian criminal code that prohibits such scams. Although they are now perpetrated globally in a variety of forms, they are most commonly associated with Nigeria and other African countries.

⁵ <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

⁶ As of January 2010, only five states (Alaska, Hawaii, Massachusetts, North Carolina and Wisconsin) require disclosure of compromises involving personal information maintained in any format including paper records.

⁷ Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR Part 30 (Office of the Comptroller of the Currency), Parts 208 and 225 (Federal Reserve system), Part 364 (Federal Deposit Insurance Corporation), Part 568 and 570 (Department of the Treasury, Office of Thrift Supervision), effective March 29, 2005.

15. Beyond the misuse of personal information, are there other data usage and protection risks that should be considered?

Yes. Other relevant risks in this area include:

- Information might be permanently lost or improperly altered, which may create customer service issues and/or limit a firm's ability to respond effectively to governmental requests for information, litigation, and other matters.
- Improper controls over information sharing can lead to regulatory violations and/or a breach of promises to consumers where companies have promised not to share – or customers have opted out of sharing – information with certain types of affiliates and third parties, even if such sharing is technically permissible under applicable laws and regulations.
- Excessive or unreasonably burdensome security measures can negatively impact a firm's profitability and/or growth goals without measurably improving protection of customer data.

16. What types of businesses have the most significant exposure to privacy risk?

While all businesses are exposed to privacy risk to some extent (for example, with regard to the need to protect sensitive information related to their employees and customers), the following types of businesses have a greater susceptibility to such risks:⁸

- Financial services organizations (e.g., banks, funds, credit card issuers, insurers, and their supporting vendors such as payment processors, web hosts)
- Marketing and retail companies
- Communication and media (e.g., online marketplace and payment websites, social networking websites)
- Educational institutions (e.g., universities, colleges)
- Healthcare and research organizations (e.g., hospitals, long-term care facilities, specialized health services)
- Governmental and quasi-governmental agencies (e.g., real estate registers, voter registers, census and opinion polls, military support)

17. What steps have lawmakers and regulators taken to address concerns about privacy?

As detailed elsewhere in this FAQ guide, the past 10 years have seen a virtual explosion in the number of U.S. laws and regulations designed to protect consumers' privacy and ensure the security of their personal information. Current standards in this area are a mix of specific, prescriptive requirements and prohibitions, together with principles-based rules that require firms to conduct their own risk assessments and implement protection programs appropriate for their circumstances. Additionally, more and more laws are either expressly establishing or implying a duty of care on the part of private organizations and governmental bodies to protect information that they collect and maintain, which at least potentially opens the door to litigation in the event that a breach occurs.

The rapid growth in the number of laws/regulations and the variety of specific requirements they impose makes this area quite difficult to understand and manage. In addition to federal regulations imposing requirements nationally, individual states have enacted statutes and regulations that impose varying standards across the country. These state statutes and regulations may impose obligations on businesses that collect information about residents of the state even though the business does not physically have a presence in that state. This patchwork of state regulations poses significant challenges to businesses with a national customer base or a multistate presence. Conducting business through the Internet has increased the reach of these resident-centric statutes.

⁸ *Managing and Auditing Privacy Risks*: <http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-guides/gtag/gtag5/>

18. What are the primary objectives of privacy legislation?

Each piece of legislation and/or regulation in this area has its own specific goals and objectives, but there are certainly common themes that exist in these requirements. The AICPA's privacy framework, which itself is based on the Organisation for Economic Co-operation and Development's (OECD) Fair Information Practices (FIPs) standard, nicely summarizes the objectives of the various types of privacy laws and regulations. Nearly all such standards impose requirements in many or most of these common areas, some of which include:

- Notice
- Choice and consent
- Security
- Access and correction

19. Why don't privacy laws protect businesses?

As a general matter, privacy laws (at least within the United States) are in place to protect the individual. Lawmakers and regulatory agencies tend to believe that businesses have a greater degree of sophistication, the ability to assess and allocate risks among themselves, and the resources necessary to protect their own sensitive information and take advantage of civil remedies available to them in the event that a breach occurs. For example, in a business-to-business transaction, the party that is putting sensitive data at risk can specify by contract that the other party will take adequate steps to protect this information, and indemnify the party at risk in the event that a breach occurs.

Such a company could also sue to recover any damages incurred as a result of a breach that was not specifically contemplated by contract under a number of broader legal theories. Businesses also have laws to protect their assets that do not necessarily apply to individuals (e.g., trade secret laws). Meanwhile, consumers do not typically have the knowledge, resources, or leverage to negotiate specific terms of service with large financial services, medical, and other providers who will have access to their sensitive information, and may be similarly limited in their ability to pursue civil remedies in the event that a breach occurs.



Discussion of U.S. Federal Privacy Laws and Regulations

Gramm-Leach-Bliley Act (GLBA)

20. What businesses are covered by the Gramm-Leach-Bliley Act (GLBA)?

The GLBA only applies to “financial institutions,” which includes institutions engaged in financial activities as described in the Bank Holding Act of 1956. This includes institutions significantly engaged in “financial activities.” In general, any business that provides financial services to consumers is covered. A broad spectrum of entities is covered, including, but not limited to, banks, savings institutions, credit unions, money services businesses, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage brokers, check-cashing businesses, businesses that wire money to and from consumers, accountants in the business of completing income tax returns, investment advisory companies, and credit counseling services.

The definition does not include, however, any person or entity engaged in financial activities that are subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act, the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971, or other secondary market institutions.

Businesses that offer both financial and nonfinancial services should consult their legal professionals regarding their compliance obligations.

21. Does the GLBA have different requirements for different types of customers?

Yes. More extensive requirements and disclosures are imposed for individuals who have ongoing customer relationships with the financial institution. However, depending upon the nature of the institution’s information-sharing practices, certain disclosures and other requirements may be imposed, even for individuals who may have had a onetime relationship with the financial institution. These differences are reflected in the different requirements for “consumers” and “customers.”

22. What personal information is protected?

GLBA governs the treatment of “nonpublic personal information” (NPI). NPI includes information that is not generally publicly available and that:

- Is provided to the financial institution by a consumer to obtain a financial product or service,
- Results from a transaction involving a financial product or service between a financial institution and a consumer, or

- A financial institution otherwise obtains in connection with providing a financial product or service.

NPI can consist of individual items of information, as well as compilations or lists of information.

Examples of NPI may include, but are not limited to:

- The simple fact that a consumer maintains a relationship with a financial institution;
- A customer's annual income, credit score or net worth;
- A customer's balance or payment history at a financial institution; or
- A list of customers who have balances in excess of a certain amount or who maintain a certain product or service at a financial institution.

The institution must have reason to believe that information is lawfully made available to the general public from widely distributed media, legally required disclosures to the general public or government records in order for the information to be considered publicly available. Information in a telephone book, in a publicly recorded document (such as a Uniform Commercial Code (UCC) financing statement) or in a securities filing is all publicly available. However, if a list of otherwise public information is compiled from a financial institution's nonpublic personal information, such as a list of customers, that list under most circumstances would be considered nonpublic.

23. What is the difference between a “consumer” and a “customer”?

A “consumer” is an individual who obtains financial products or services from a financial institution that are primarily used for personal, family or household purposes; however, the individual does not have an ongoing relationship with the institution. In contrast, a “customer” is a type of consumer who also is obtaining financial products or services to be used primarily for personal, family or household purposes, and who has an ongoing relationship with a financial institution through which they are provided a financial product or service.

For example, under the GLBA, a consumer would be a person who is applying for a loan but has not yet obtained a loan or lending product or who cashes checks with a check-cashing company. A customer would be a person who has a checking account or who opens a credit card account with a financial institution or obtains a loan from a mortgage lender.

It is important to note that the GLBA definitions of consumer and customer only apply to individuals; businesses and individuals who obtain financial products or services for business purposes, therefore, are not considered consumers or customers for the purposes of the GLBA.

24. Does the GLBA mandate a privacy policy notice?

Yes. Every financial institution must develop initial and annual privacy policy notices that must be provided to consumers or customers. Developing and sending customers a revised privacy policy notice may be necessary when a financial institution changes its information-sharing practices.

25. What must a privacy policy notice include?

All privacy policy notices must be written in clear, concise sentences, using plain language and active voice. They must also be designed to call attention to the nature and significance of the information contained in the notice. Under the GLBA, there are four types of privacy policies:

Initial or Annual Notice: The required contents for the Initial and Annual Notices are the same, and must contain, to the extent applicable based on each financial institution's information-sharing practices:

- Categories of nonpublic information (NPI) that the financial institution collects;
- Categories and examples of NPI that the financial institution discloses;
- Categories and examples of affiliates and nonaffiliated third parties to whom the financial institution discloses NPI;
- Explanation of the right to opt out;
- Disclosures required under the Fair Credit Reporting Act for financial institutions;
- The financial institution's practices and policies for protecting the confidentiality and security of NPI;
- If the financial institution discloses NPI about its former customers, the categories of NPI disclosed, and the categories of affiliates and nonaffiliated third parties to whom it discloses NPI;

- If the financial institution discloses NPI to a nonaffiliated third party that is a service provider or joint marketing partner of the institution, a separate statement of the categories of NPI disclosed to the third party and a statement about the relationship between the institution and the third party; and
- If the financial institution discloses NPI under any other exceptions authorized by the GLBA, a statement that these disclosures are permitted by law.

Short-Form Notice: Should be used instead of an Initial Notice when the notice is being given to a consumer who is not a customer. This Short-Form Notice should inform the consumer that the financial institution's full privacy policy is available upon request and direct the consumer to a reasonable means by which they may get the full notice.

Simplified Notice: Should be used when a financial institution does not disclose any NPI about its customers to any affiliates or nonaffiliated third parties. This Simplified Notice should contain a list of the categories of NPI that are collected, a statement explaining the institution's policies and practices for safeguarding NPI, and a statement explaining that the institution does not disclose any NPI to affiliates or nonaffiliated third parties, except as permitted by law.

Revised Notice: Should be used if a financial institution changes any of its policies and practices for the disclosure of NPI to nonaffiliated third parties, making the existing privacy policy notice no longer accurate. This Revised Notice should contain a new notice that accurately reflects the new changed policies, and provides a new opt-out notice and a reasonable means to opt out.

On December 1, 2009, six agencies published the Final Model Privacy Form Under the Gramm-Leach-Bliley Act. This Final Rule allows for the use of a simplified model form for providing privacy notices required under the GLBA. The Final Rule was published in the Federal Register in Vol. 74, No. 229, p. 62890.

26. When does a financial institution need to provide a copy of a privacy policy?

A financial institution must provide its privacy policy in the following instances (for a detailed description of each of the following notices, please see Question 25):

Initial Notice: Must be given to a customer at the time that the customer relationship is established, or earlier. An Initial Notice must be given to a consumer prior to sharing the consumer's NPI.

Annual Notice: Must be given to a customer a least once in any period of 12 consecutive months, for the duration of the customer relationship.

Short-Form Notice: Can be given to a consumer who is not a customer, in the place of an Initial Notice, and must be given prior to sharing the consumer's NPI. A Short-Form Notice should give the consumer a reasonable opportunity to opt out before any of their NPI is shared outside of the exceptions permitted by the regulation.

Simplified Notice: Must be given to a customer at the time that the customer relationship is established, or earlier.

Revised Notice: Must be given to consumers, customers, and former customers whenever the financial institution changes any of its policies and practices for the disclosure of NPI to nonaffiliated third parties, outside of the exceptions set forth in §§ 13, 14 and 15 of the Regulation.

27. What is an "opt-out" notice and when must a financial institution provide it?

An opt-out notice usually must be given by a financial institution to a consumer before it can disclose the consumer's NPI to a nonaffiliated third party (see Question 28 for circumstances where an opt-out is not required). The opt-out notice must inform the consumer that the financial institution discloses NPI about consumers to nonaffiliated third parties and give the consumer a reasonable opportunity to opt out of the disclosure of their NPI before the financial institution discloses such information to a nonaffiliated third party. To meet the requirement of a reasonable opportunity to opt out, the financial institution can provide the consumer with a toll-free phone number, a form with mailing information, or an e-mail (if the consumer has agreed to receive notices electronically) to opt out. If either a required opt-out notice is not given or if the consumer exercises the opt-out, the financial institution cannot disclose the consumer's NPI to a nonaffiliated third party.

28. With whom may a financial institution share personal information without providing an opt-out?

Under the GLBA, a financial institution may disclose certain types of NPI to any of its affiliates without providing an opt-out, but the Affiliate Marketing Rule imposes opt-out obligations as noted in Question 89. An affiliate is any company that controls your company, is under the control of your company, or along with your company is under the common control of another company.

There are several exceptions to the GLBA's opt-out requirement that allow a financial institution to disclose a consumer's NPI to a nonaffiliated third party without providing the consumer with the opportunity to opt out. Such exceptions include disclosures:

- To a third-party service provider that provides services to the financial institution and with whom the financial institution has signed a contract prohibiting the use of the NPI other than for the purpose disclosed;
- To other financial institutions that the financial institution has entered into joint marketing agreements with and with whom they have signed a contract prohibiting the use of the NPI other than for the purpose disclosed;
- To insurance rate advisory organizations, people assessing compliance with industry standards, and the financial institution's attorneys, accountants or auditors;
- To a consumer reporting agency, law enforcement entities, and self-regulatory groups (to the extent permitted by law);
- Made with a consumer's consent;
- To protect the security of records, to prevent potential fraud, for required institutional risk control, or for resolving consumer inquiries;
- To comply with a subpoena, other judicial process, or federal, state or local laws; and
- Made in connection with the servicing or processing of a financial product or service that a consumer requests or authorizes, the maintaining or servicing of a consumer's account, or a proposed securitization or secondary market sale.

A financial institution may not disclose, however, either directly or through an affiliate, a consumer's account number to a nonaffiliated third party for use in marketing.

29. Are there regulations governing the GLBA?

Yes, there are eight government agencies that have issued regulations governing the GLBA. They are the Office of the Comptroller of the Currency of the Department of Treasury, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision of the Department of Treasury, the National Credit Union Administration, the Federal Trade Commission, the Commodity Futures Trading Commission, and the Securities and Exchange Commission.

30. May a financial institution share personal information with its vendors?

Except in cases where an opt-out is not required (see Question 28), a financial institution may not disclose NPI to a nonaffiliated third party unless the consumer has been provided with and has elected not to exercise the right to opt out as to that third party. However, the financial institution may disclose such NPI to a vendor that is also the financial institution's affiliate, subject to the requirements and restrictions of the Fair Credit Reporting Act described elsewhere in this guide.

31. Does the GLBA impose other requirements?

Yes. For example, financial institutions covered by the GLBA are also required to comply with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, which requires financial institutions to establish a security breach response program and, in general, to notify affected customers when a breach occurs. In addition, financial institutions are required to maintain certain security policies and procedures pursuant to the Interagency Guidelines Establishing Information Security Standards. Other regulations imposed by the agencies listed in Question 29 may also apply to financial institutions (such as Identity Theft Red Flags Rules), depending on their activities. Finally, financial institutions may be required to comply with the Health Insurance Portability and Accountability Act (HIPAA) (see the following section) under certain circumstances. Please consult your legal professional.

32. What are the penalties for violating the GLBA?

The penalties for violation of the GLBA can be severe. A financial institution can be fined up to \$100,000 per violation. In addition, the officers and directors can each be fined up to \$10,000 for each violation. Criminal penalties are also available to enforce the statute. Criminal penalties include fines or imprisonment up to 5 years, or both, and in certain circumstances (where GLBA is violated at the same time another federal law is violated or where the GLBA is violated as a part of a pattern of any illegal activity involving more than \$100,000 within a 12-month period) the criminal sanctions can be doubled.

Health Insurance Portability and Accountability Act (HIPAA)

33. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996, and is codified in Title 42, Section 1320d of the U.S. Code. HIPAA's purpose is to improve portability and continuity of health insurance coverage, reduce healthcare fraud and abuse, reduce the costs and administrative burdens of healthcare, and protect the privacy of personal health records by protecting the security and confidentiality of healthcare information. The primary impact of HIPAA's privacy provisions is to require "covered entities" and their "business associates" to comply with extensive documentation requirements and to adhere to a comprehensive set of policies, procedures and compliance measures regarding the privacy and security of protected health information (PHI).

34. How did HITECH change HIPAA?

On February 17, 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA). A significant portion of the economic stimulus legislation is comprised of the Health Information Technology for Economic and Clinical Health Act (HITECH or the HITECH Act). Subtitle D of HITECH amends HIPAA to impose substantial new obligations on both covered entities and their business associates. Prior to HITECH, business associates were only contractually obligated to comply with HIPAA and its implementing regulations through "Business Associate Agreements." HITECH changed this, and now business associates are directly accountable to comply with a number of HIPAA's requirements. HITECH also enhanced HIPAA's enforcement provisions, increased the limitations on use of PHI, restricted the sale and marketing of PHI, and imposed new breach notification requirements for unauthorized disclosures of unsecured PHI.

35. Are there regulations that govern HIPAA?

Yes. While there are several sets of regulations that fully implement HIPAA, two rules are typically of most interest to providers: the Privacy Rule and the Security Rule. The Privacy Rule created national standards to protect the privacy of personal health information. The Security Rule created national standards for the security of electronic healthcare information. The HIPAA Privacy Rule, formally titled *The Standards for Privacy of Individually Identifiable Health Information*, was published in December 2000, later revised in August 2002, and is codified at Title 45, Parts 160 and 164, Subparts A and E of the Code of Federal Regulations. The Privacy Rule protects against the improper use or disclosure of PHI, which is defined as individually identifiable health information that is (1) transmitted by electronic media, (2) maintained in any electronic media, or (3) transmitted or maintained in any other form or medium. The Privacy Rule increases patient rights and limits a covered entity's or business associate's ability to use and/or disclose PHI. The U.S. Department of Health and Human Services (HHS) adopted the HIPAA Security Rule in February 2003. The Security Rule protects the confidentiality and availability of health information in electronic form, and it is codified at Title 45, Parts 160, 162, and 164 of the Code of Federal Regulations. Regulations issued pursuant to HITECH with respect to enforcement and breach notification can be found at 74 Federal Register 42740 (August 2009).

36. Who has to comply with the HIPAA Privacy Rule?

"Covered entities" must comply with the Privacy Rule, and business associates must comply with specified portions of the Privacy Rule.

Covered entities include (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers who transmit health information in electronic form in connection with certain transactions.

Health plans are individual or group plans that provide or pay the cost of medical care and include health insurance companies, HMOs, company health plans, and government programs such as Medicare, Medicaid, and military and veterans' healthcare programs. A health plan does not include a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan or a government program whose principal purpose is not to provide or pay the cost of healthcare (e.g., food stamp programs), directly provide healthcare (e.g., a community health center), or make grants to fund the direct provision of healthcare.

A healthcare clearinghouse is an entity that receives health information from a covered entity in a nonstandard format and processes the information into a standard format, or receives a standard transaction from a covered entity and processes the information into a nonstandard format for another entity. Healthcare clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches, if these entities perform clearinghouse functions.

Healthcare providers are providers of hospital, skilled nursing, rehabilitation, home health or hospice services, providers of medical or health services (e.g., physicians, dentists, and other practitioners), and any other person who or organization that furnishes, bills, or is paid for healthcare services in the normal course of business. To be considered a "covered entity," the healthcare provider must electronically transmit health information in connection with claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the Secretary of the U.S. Department of Health and Human Services has adopted standards under HIPAA. A healthcare provider is a covered entity regardless of whether it transmits these transactions directly or uses a billing service or other party to do so on its behalf.

"Business associates" of covered entities are entities or individuals who perform functions on behalf of a covered entity or who create, receive, or have access to protected health information maintained by a covered entity (a more in-depth discussion of the business associate relationship can be found in Question 39). Under the HITECH Act, business associates who violate the core privacy terms of their business associate agreements with a covered entity will be in direct violation of the Privacy Rule.

37. What does a HIPAA privacy policy include?

HIPAA requires covered entities to document their organizational privacy policies and procedures. The following should be included in a privacy policy:

Uses and Disclosures

- Procedures for the use and disclosure of protected health information (PHI) for treatment, payment, or healthcare operations purposes and other disclosures (e.g., disclosure to oversight agencies, law enforcement);
- A description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without an individual's written authorization;
- If a use or disclosure is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law;
- For each purpose described, the description must include sufficient detail to place an individual on notice of the permitted or required uses and disclosures; and
- A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.
- Procedures for the use and disclosure of PHI to personal representatives when patients are legally or otherwise incapable of exercising their rights;
- Business associate procedures;
- Level(s) of employee access to PHI and the procedures for documenting and monitoring such access;
- Procedures for responding to patient requests to amend PHI;
- Procedures for responding to requests for patient medical records, whether the request originates from a patient, a third party (e.g., insurance company), or through the legal system (e.g., subpoena);
- Plans for responding to a privacy or security breach;
- Training requirements for new hires; and

- The processes used to inform patients of their rights of access to or modification of their PHI (a “Notice of Privacy Practices” must be available to anyone who asks for it and must be given to any individual for whom the covered entity processes or handles PHI).

Notice of Privacy Practices

Individual Rights

The privacy notice must contain statements regarding the following individual rights with respect to PHI and a brief description of how to exercise the rights:

- The right to request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction;
- The right to receive confidential communications of PHI;
- The right to inspect and copy PHI;
- The right to amend PHI;
- The right to receive an accounting of disclosures of PHI; and
- The right of an individual, including an individual who has agreed to receive the notice electronically, to obtain a paper copy of the notice from the covered entity upon request.

Covered Entity’s Legal Duties

The privacy notice must contain:

- A statement that the covered entity is required to maintain the privacy of PHI and provide individuals with its privacy notice; and
- A statement that the covered entity is required to abide by the terms of the privacy notice currently in effect.

Other

The privacy notice must include a header or otherwise prominently display the following statement: “This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.”

In addition, the notice should be written in plain language and include statements regarding an individual’s right to complain, the complaint procedure, and the effective date of the privacy notice.

If a covered entity wishes to contact individuals to provide appointment reminders or information about treatment alternatives, for its own fundraising activities, or if a group health plan, a health insurance issuer, or HMO with respect to a group health plan wants to disclose PHI to the sponsor of the plan, it must include such statements in its privacy notice or it is prohibited from using or disclosing PHI for such activities without authorization. Further, a covered entity may change a privacy practice if it reserves the right to do so in its privacy notice, states that the modified terms will apply to all PHI that it maintains, and describes how it will provide individuals with the revised notice.

38. When do covered entities need to provide a copy of a privacy policy?

A covered entity must provide a copy of its privacy notice to *any* person who requests it, regardless of whether the person is a current patient or enrollee. In addition, depending upon the covered entity’s classification, it is subject to the following additional notice requirements.

Health Plans

A health plan must provide a copy of its privacy notice:

- At the time of enrollment to new enrollees;
- Within 60 days of a material revision to its privacy notice, to individuals then covered by the plan; and
- At least once every three years to individuals then covered by the plan regarding the availability of the notice and how it may be obtained.

No specific method of notice is required, and a health plan does not have to obtain an acknowledgement from the individual that a copy of the privacy notice was received.

Healthcare Providers

A covered healthcare provider must provide a copy of its privacy notice no later than the date the provider first delivers services (including electronically delivered services) to the individual after the compliance date. However, in an emergency treatment situation, the privacy notice may be provided as soon as reasonably practicable after delivering treatment. Except in an emergency treatment situation, a covered healthcare provider must also make a good faith effort to obtain written acknowledgment from the individual that a copy of the privacy notice was received. In addition, if a covered healthcare provider maintains an office or other facility where services are physically delivered, the notice must be available at that site for individuals to request and take and must be posted in a clear and prominent location.

Electronic Notice

A covered entity that maintains a website that provides information about customer services or benefits must prominently post its privacy notice on the website and make it available electronically through the website. A covered entity may also send its privacy notice to an individual by e-mail, if there is a current agreement in effect with the individual permitting electronic notice.

39. With whom may covered entities share protected health information?

Covered entities may disclose PHI for treatment, payment, or healthcare operations purposes. Covered entities may also disclose PHI to business associates. Business associates are those who perform functions on behalf of a covered entity and create, receive, or have access to PHI maintained by the covered entity. More specifically, a “business associate” is a person or entity (who/which may be another covered entity), other than a member of the covered entity’s workforce, that performs, or assists others in performing, on behalf of the covered entity, a function or activity that entails the use or disclosure of PHI obtained from the covered entity or another business associate of the covered entity. Relevant “functions” include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, repricing, practice management, and other functions regulated by the HIPAA Privacy Rule.

Essentially, a business associate relationship arises when the right to use or disclose the PHI belongs to the covered entity, and another person is using or disclosing the PHI to perform a function or activity on behalf of the covered entity. Business associates include vendors to covered entities that provide certain defined services (e.g., accounting, legal, consulting, and/or financial services) and have access to PHI. Business associate agreements that define the nature and scope of the information-sharing arrangements between the covered entity and the business associate should be maintained for each business associate. The HITECH Act extends application of specified portions of the Privacy Rule and the Security Rule directly to business associates. In addition to complying with the Privacy Rule and the Security Rule, business associates also are subject to HIPAA’s civil and criminal penalty provisions.

Covered entities can disclose PHI for law enforcement purposes, to avert a serious threat to health or safety, or for other specific purposes. Covered entities can also disclose information about decedents to coroners, medical examiners, and funeral directors. If a covered entity uses, discloses, or requests PHI, it must ensure that it complies with HIPAA’s “minimum necessary” requirement. The “minimum necessary” requirement provides that, when using, disclosing, or requesting PHI from another covered entity, a covered entity must to the extent practicable limit the disclosure of PHI to a “limited data set” as defined by HIPAA. This “limited data set” is partially de-identified information that does not contain direct identifiers such as names, addresses and Social Security numbers. The covered entity making the disclosure is required to determine which information constitutes the “minimum necessary” for disclosure. The covered entity may not rely on the requesting party’s determination that it has only requested the minimum necessary. However, the “minimum necessary” requirement does not apply to:

- Disclosures to or requests by (but not uses by) a healthcare provider for treatment purposes;
- Uses or disclosures made to an individual at his or her request, and disclosures upon an individual’s request for access or an accounting of disclosures;
- Uses or disclosures made pursuant to an authorization or that are required by law;
- Disclosures made to the secretary for compliance and/or enforcement purposes; or
- Uses or disclosures that are required for compliance with applicable regulations regarding HIPAA’s standards regarding the uniformity of data sets in healthcare transactions.

To disclose PHI for purposes other than treatment, payment, or healthcare operations, a covered entity must obtain patient authorization. Authorization can include permission to disclose PHI to third parties generally, or for specific purposes such as marketing. Additionally, covered entities may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation, including payment of claims.

HITECH prohibits the sale of PHI by a covered entity or business associate without a valid authorization from an individual. Sale without authorization is allowed in the following instances:

- For public health activities;
- For research activities for which the price charged reflects the cost of preparation and transmittal of the data;
- For the treatment of the individual;
- Related to the sale, transfer, or merger of all or part of a covered entity;
- To provide an individual with a copy of his/her PHI; or
- Deemed necessary and appropriate by the Secretary of HHS.

HHS must issue regulations relating to the sale of PHI prior to August 17, 2010. The regulations will become effective six months after they are issued.

40. Do covered entities need to get consent to share protected health information with data processing vendors?

If the sharing of PHI with data processing vendors is for the purpose of treatment, payment, or healthcare operations, then consent is not needed. However, consent to share PHI with a data processing vendor must be obtained for any other purpose. If the data processing vendor is a business associate, and a business associate agreement is on file, then consent is not needed. The uses and disclosures permitted or required for data processing vendors may be narrower than what would apply to the covered entity under the HIPAA Privacy Rule. However, the uses and disclosures may not be broader than what would apply to the covered entity, unless it is for the proper management and administration of the business associate or to provide data aggregation services relating to the healthcare operations of the covered entity.

An agreement is not required for: (1) disclosures by a covered entity to a healthcare provider with regard to the individual's treatment; (2) disclosures to a plan sponsor by the group health plan, or a health insurance issuer or HMO with respect to the group health plan, if the plan documents restrict the uses and disclosures of such information in accordance with the requirements of the HIPAA Privacy Rule; or (3) an agency administering a government health plan that provides public benefits and another agency ("B") in order to collect and share PHI if B determines or collects the PHI used to determine the eligibility for, or enrollment in, the health plan, and the joint activities of the agencies are authorized by law.

As discussed above, neither covered entities nor business associates may directly or indirectly receive any form of payment in exchange for PHI unless a valid authorization from the individual who is the subject of the PHI is given. The authorization must include an express specification that the PHI may be sold by the covered entity or business associate.

41. What document retention obligations are imposed by HIPAA?

Covered entities must retain the following documentation in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later:

- Policies and procedures;
- A communication that the HIPAA Privacy Rule requires to be in writing; and
- An action, activity, or designation that the HIPAA Privacy Rule requires to be documented. For example, a covered entity must document compliance with notice requirements by retaining copies of the notices it has issued and, if applicable, any written acknowledgments that the notice was received or documentation of good faith efforts to obtain such written acknowledgment.

An accounting of disclosures, including disclosures of PHI for treatment, payment, or healthcare operations, must be maintained for three years.

42. What requirements apply when there is a breach of protected health information?

Responding to a Privacy or Security Breach

Under HIPAA, covered entities and business associates must notify affected individuals of any breach of unsecured PHI. In determining whether a breach of unsecured PHI has occurred, covered entities and their business associates should analyze the following:

- (1) **Determine whether the use or disclosure of unsecured PHI violates the HIPAA Privacy Rule.** For an acquisition, access, use, or disclosure of unsecured PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified, it is not considered to be PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a breach under the notification requirements of the Act and the Rule.
- (2) **Analyze whether there is a use or disclosure that compromises the security and privacy of PHI.** HHS clarifies that a use or disclosure that “compromises the security and privacy of PHI” means a use or disclosure that “poses a significant risk of financial, reputational, or other harm to the individual.” Thus, in order to determine whether a breach has occurred, covered entities and business associates should conduct a risk assessment to determine whether the potential breach presents a significant risk of harm to individuals as a result of an impermissible use or disclosure of PHI.
- (3) **Assess whether an exception to the definition of “breach” applies.** The following three situations are excluded from the definition of “breach” under the Act:
 - (i) The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
 - (ii) The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at an organized healthcare arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
 - (iii) An unauthorized disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Notification Requirements to Individuals or Media in the Event of a Breach

The HITECH Act added significant requirements that apply in the event of certain breaches of the privacy of PHI. Breach notifications are triggered by the “discovery” of the breach of unsecured PHI. A breach is treated as “discovered” by a covered entity as of the first day the breach is known, or reasonably should have been known, to the covered entity. Given that knowledge of a breach may be imputed, a covered entity should implement reasonable breach discovery procedures.

- **Notification to Individuals.** A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach, without unreasonable delay and in no case later than 60 calendar days after the date the breach was first discovered by the covered entity. HIPAA specifies the content requirements and the methodology required for providing breach notices. For covered entities that do not have sufficient contact information for 10 or more affected individuals, the Rule requires that “substitute notice” be provided as soon as reasonably possible. “Substitute notice” is provided via a posting for a period of 90 days on the home page of the covered entity’s website or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In such instances, the covered entity is also required to have an active toll-free number for 90 days so that an individual may determine whether his or her unsecured PHI may be included in the breach.
- **Notification to Media.** If a covered entity discovers a breach affecting more than 500 residents of a state or jurisdiction, the covered entity must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the covered entity.

- **Notification to HHS.** If the information of more than 500 individuals is involved in the breach, regardless of whether the breach involved more than 500 residents of a particular state or jurisdiction, then the covered entity must notify HHS concurrent with the individual notifications. For breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such breaches and annually submit the log to HHS.
- **Notification by a Business Associate.** Following a business associate's discovery of a breach of unsecured PHI, the business associate is required to notify the covered entity of the breach so that the covered entity can, in turn, notify the affected individuals. To the extent possible, the business associate should identify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. Such notice should be given without unreasonable delay, but no later than 60 days following discovery of a breach.
- **Delay Required by Law Enforcement.** The Act provides that a breach notification may be delayed if a law enforcement official determines that such notification would impede a criminal investigation or cause damage to national security.

Breaches of Unsecured PHI

The breach notification rules do not apply to all breaches of PHI, but instead apply only to breaches of PHI that are unsecured. "Unsecured" PHI is information that is not secured through the use of technologies or methodologies that render the PHI "unusable, unreadable, or indecipherable to unauthorized individuals," either by encryption or destruction in accordance with specifications issued by the National Institute of Standards and Technology (NIST). So, if a covered entity and its business associates use the required methodologies to encrypt or destroy PHI, they will not be subject to the reporting and notice requirements imposed by the HITECH Act.

Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA)

43. What is the Fair Credit Reporting Act?

The Fair Credit Reporting Act (FCRA) regulates information collected and distributed by consumer reporting agencies. The FCRA grants statutory rights to patrons of consumer reporting agencies and the public in general and protects individuals by promoting the accuracy, fairness, and privacy of the information contained in consumer reporting agency files.

The FCRA protects consumers by limiting the information that a consumer reporting agency can include in a consumer credit report. In general, a report may *not* contain:

- Bankruptcies that are more than 10 years old;
- Civil suits that are more than seven years old, or in which the statute of limitations has expired, whichever is longer;
- Paid tax liens which, from the date of payment, are more than seven years old; or
- An account placed for collection or charged to profit and loss, or any other adverse item of information, that is more than seven years old.

However, the foregoing restrictions do not apply to:

- A credit transaction involving, or which may reasonably be expected to involve, a principal amount of US\$150,000 or more;
- The underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of US\$150,000 or more; or
- The employment of any individual at an annual salary which equals, or which may reasonably be expected to equal, US\$75,000 or more.

The FCRA also restricts the disclosure of medical information, except in limited circumstances, and addresses the issue of identity theft. For example, if a consumer gives notice that identity theft may have occurred, the consumer reporting agency must, among other requirements, include a fraud alert in the consumer's file and provide that alert with any credit score generated.

Finally, the FCRA protects consumers by requiring transparency on the part of the consumer reporting agency. Under the FCRA, agencies must allow a consumer to access his or her file upon request, and each consumer is entitled to one free disclosure every 12 months. In addition, if any information that is provided by a consumer reporting agency is disputed

by the consumer and determined to be inaccurate, incomplete, or unverifiable, the agency must remove or correct the information, usually within 30 days.

Please note that the FCRA frequently uses the word “person” to refer to the entity providing credit reports. “Person,” for purposes of the FCRA, means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

44. To whom does the FCRA apply?

The FCRA applies to “consumer reporting agencies” and any person requesting, handling, or using consumer reports. In addition, the FCRA imposes obligations on persons accepting a credit card for payment of goods or services (requiring truncation of the credit card number on the printed receipt) and certain rules and regulations promulgated under the FCRA apply to a wide variety of persons and entities, such as the Affiliate Marketing Rule (see Question 89 and the identity theft red flags rules questions discussed below).

45. What is a “consumer reporting agency”?

A “consumer reporting agency” refers to any entity that, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). The major (or “national”) consumer reporting agencies are Equifax, Experian, and TransUnion.

46. What constitutes consumer report information?

Consumer report information is information that has any bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected in whole or in part to assist in establishing the consumer’s eligibility for: (1) credit or insurance to be used primarily for personal, family, or household purposes; (2) employment purposes; or (3) any other purpose authorized by the FCRA.

Consumer report information generally does not include:

- Any information regarding only the transactions between the person making the report and the consumer;
- Communication of the foregoing information among affiliates (except, for example, for purposes determining implication of the Affiliate Marketing Rule);
- Communication of other information among affiliates, as long as the consumer knows of, and had the opportunity to veto, such communication;
 - The foregoing is also known as affiliate sharing, which is addressed in more detail in Question 89.
- Any authorization or approval of an extension of credit by the issuer of a credit card or similar device; or
- Any information regarding a person’s approval or denial of an extension of credit to a consumer, which was initiated at the request of a third party, provided that the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the necessary disclosures and communications to the consumer. Typical extensions of credit include a home loan or a request to increase a credit card limit, but it may also include any services that are rendered prior to payment.

47. Are there any instances where the exclusions for consumer report information do not apply?

The exclusions in the previous answer do not apply in limited circumstances, such as to information disclosed to any affiliate, if the information is:

- Medical information;
- An individualized list or description based on the payment transactions of the consumer for medical products or services; or

- An aggregate list of identified customers based on payment transactions for medical products or services.

“Medical information” is information, whether oral or recorded, from a healthcare provider or the consumer, that relates to the health or condition of the consumer, or a provision or the payment for the provision of healthcare to the consumer. “Medical information” does not include basic information about a consumer’s age, gender, address, insurance policy, or any other information that does not relate to the physical, mental, or behavioral health or condition of the consumer.

Further, consumer report information does not include communications made to an employer in connection with an investigation of suspected misconduct relating to employment or compliance with federal, state, or local laws, the rules of a self-regulatory organization, or any pre-existing written policy of the employer. In this situation, the communication must not be made to investigate a consumer’s credit worthiness, credit standing, or credit capacity. Further, the communication must not have been provided to any person other than: (1) the employer or an agent of the employer; (2) any federal or state officer, agency, or department, or any officer, agency, or department of a unit of general local government; (3) any self-regulatory organization with regulatory authority over the activities of the employer or employee; or (4) as otherwise required by law.

Finally, consumer report information does not include “excluded communications.” A communication is an “excluded communication” if it is made to a prospective employer to procure an employee or to procure the opportunity for a natural person to work for the employer, is only used for these purposes, is made by a person who regularly handles such procurement, and if: (1) the consumer consents to the nature and scope and the making of the communication before the employer collects any information to make the communication or makes the communication; and (2) if the consent is given orally, and written confirmation of such consent is provided within three days after the consent is given. During this process, the employer may not ask any questions that would violate federal or state law. Further, the person who makes the communication must disclose to the consumer in writing, within five days after receiving any request from the consumer for such disclosure, all of the information in the consumer’s file (except the sources of any information acquired solely to make the communication, which is not used for any other purpose). The person who makes the communication must inform the consumer in writing of his or her right to the foregoing disclosure.

48. Who may request a consumer report?

There are limitations on who may request a consumer report and how a consumer report or the information in it may be used. Strict compliance with the FCRA requirements is required and penalties can be severe for violations. The statute permits the following people and/or entities to request a consumer report:

- A consumer, in regard to his or her own consumer report file (each consumer is entitled to one free disclosure every 12 months);
- A court having jurisdiction;
- An individual, if the request is made in accordance with the written instructions of the consumer to whom the report relates;
- A person who intends to use the information:
 - In connection with the extension of credit, or review or collection of an account;
 - For employment purposes (provided the consumer has provided consent);
 - In connection with the underwriting of insurance;
 - In connection with a determination of the consumer’s eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant’s financial responsibility or status; or
 - As a potential investor or servicer, or current insurer, in connection with the valuation of, or an assessment of, the consumer’s existing credit obligations.
- A governmental agency authorized to conduct investigations regarding international terrorism;
- The Federal Bureau of Investigation (FBI), to protect against international terrorism or clandestine intelligence activities;
- A victim of identity theft (this information should be provided free of charge once the victim has verified his or her identity and the fact of identity theft); and
- All others with a legitimate business purpose. The definition of “business purpose” is discussed in Question 49.

A business entity does not have to provide a consumer report if the FCRA does not require disclosure, the entity does not have a high degree of confidence in the true identity of the person requesting the information, the person requesting the information is misrepresenting a material fact, or the information requested is regarding a consumer's visit to websites or online services.

49. What constitutes a “business purpose” for requesting a consumer report?

A business purpose includes requesting the information for use in connection with a credit transaction (extension of credit, or review or collection of an account); for employment purposes; in connection with the underwriting of insurance involving the consumer; in determining the consumer's eligibility for a license or other benefit granted by a governmental instrumentality that is required to consider the applicant's financial status; as a potential investor or servicer, or current insurer, to assess the existing credit obligations of the consumer; or for other legitimate business needs in connection with a business transaction that is initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account.

In a non-binding opinion, the Federal Trade Commission (FTC) explained the concept of a legitimate business need in connection with a business transaction initiated by a consumer, as related to the situation where a consumer approaches a salesperson at an automobile dealership. If a consumer approaches a salesperson and asks about a vehicle's price, available financing options, or even asks to test drive the vehicle, the FTC noted that this might just be comparison shopping rather than an actual initiation by the consumer to purchase or lease the vehicle. Therefore, there is probably no legitimate business need for the salesperson to request a consumer report. If the salesperson actually needs the report before talking about financing with the consumer, then he or she must explain this to the consumer and get written permission before requesting the report. A salesperson may only obtain a credit report without permission from the consumer when it is clear to both the consumer and the dealer that the purchase or lease of a vehicle is under way. Only then does a legitimate business need exist.

In other, more unusual cases, consumer reporting agencies may be compelled to provide credit information about a consumer at the request of an agency for the business purpose of administering a state plan related to a child support award, or the Federal Deposit Insurance Corporation or National Credit Union Administration to assist in the liquidation of a (possibly failing) insured depository institution or insured credit. In addition, a credit agency must comply with a request from the head of a state or local child support enforcement agency, as long as these bodies certify that: the report will be used to determine the consumer's ability to make child support payments or the appropriate level of such payments; the consumer is the actual parent to the child (if state laws require); notice has been sent to the consumer at least 10 days prior to the request; and the report will be kept confidential and not used for any other purpose other than the aforementioned.

50. What is a security freeze?

A security freeze prohibits consumer reporting agencies from disclosing a consumer's reporting file or credit score, unless the consumer authorizes such access. In theory, a security freeze should prevent identity theft thieves from opening a new line of credit because most businesses will not issue new credit without first reviewing an applicant's credit report or credit score. A large majority of states have adopted security freeze laws, and the “big three” consumer reporting agencies – Equifax, Experian and TransUnion – offer the service in each state regardless of whether a state security freeze law has been adopted. A consumer's current creditors are exempt from the security freeze, as are law enforcement agencies and certain governmental agencies that need the reports for investigations and other statutory responsibilities.

51. When is a security freeze permitted?

Generally, any consumer may request that a security freeze be placed on his or her credit file at any time. However, security freeze laws are state-specific, and the law in the applicable state should be reviewed to determine each state's specific requirements.

52. Can a charge be imposed for freezing or unfreezing a consumer report?

Yes. Generally, the fee to place, temporarily lift, or remove a security freeze is between \$5 and \$10, but this cost varies from state to state. An individual requesting a security freeze should check the cost in his or her individual state. Most states provide a security freeze to identity theft victims for free.

53. What is an investigative consumer report?

An investigative consumer report provides information about a consumer's character, general reputation, personal characteristics, or mode of living. This information is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he or she is acquainted or may have knowledge concerning any such items of information. However, such information does not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

54. Who may request an investigative consumer report?

Although not specifically addressed in the FCRA, the FTC indicated in a non-binding opinion letter that generally, an investigative consumer report may be requested by an employer or other user who has a permissible purpose to obtain the report.

The FCRA does provide that an investigative consumer report may not be prepared on any consumer unless written notice is mailed to the consumer, no later than three days after the date the report was requested, disclosing that the report will include information as to the consumer's character, general reputation, personal characteristics, and mode of living, and that the consumer has the right to request additional disclosures. The additional disclosures include: the consumer's right to obtain a copy of the report; the frequency and circumstances in which a consumer may obtain a free credit report; the consumer's right to dispute information in his or her file; the right to obtain a credit score and an explanation of how to obtain a credit score; and the method by which a consumer can contact and obtain a consumer report from a consumer reporting agency. These additional disclosures must be made in writing and mailed, or otherwise delivered, to the consumer no more than five days after the consumer's request was actually received or such report was first requested, whichever is later.

A consumer reporting agency may only provide an investigative consumer report to a person who has certified that the initial disclosures have been made and that the person will comply with the additional disclosure if requested.

55. FCRA provides certain rights when adverse action is taken based on consumer report information. What is an "adverse action"?

An "adverse action" means (1) a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested (excluding a refusal to extend additional credit under an existing credit arrangement where the applicant is delinquent or otherwise in default, or where such additional credit would exceed a previously established credit limit); (2) a denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance; (3) a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee; (4) a denial or cancellation of, an increase in any charge for, or any other adverse or unfavorable change in the terms of, any license or benefit described in the FCRA; and (5) an action taken or determination that is: (a) made in connection with an application that was made by, or a transaction that was initiated by, any consumer, or in connection with a review of an account under the FCRA; and (b) adverse to the interests of the consumer.

56. When do users of consumer reports have to give notice of an adverse action?

If any person takes any adverse action against a consumer that is based in whole or in part on a consumer report, the person must provide oral, written, or electronic notice to the consumer of the adverse action, the consumer's right to obtain a free copy of the report within 60 days of receiving notice of the adverse action, and the consumer's right to dispute the accuracy or completeness of any information in a consumer report furnished by the consumer reporting agency. In addition, the person must provide to the consumer orally, in writing, or electronically the name, address, and telephone number of the consumer reporting agency (including a toll-free telephone number established by the agency if the agency compiles and maintains consumer files on a nationwide basis) that furnished the report to the person, and a disclaimer that the agency cannot explain why the decision to take the adverse action was made because the agency did not make the decision.

In the employment setting, before a person takes an adverse action against a prospective employee based in whole or in part upon a consumer report, the person must give the consumer a copy of the report and describe the following rights in writing: the consumer's right to obtain a copy of the report; the frequency and circumstances in which a consumer may obtain a free credit report; the consumer's right to dispute information in his or her file; the right to obtain a credit score and an explanation of how to obtain a credit score; and the method by which a consumer can contact and obtain a consumer report from a consumer reporting agency. This information will be provided to the employer by the consumer reporting agency, as a condition for it to provide reports for employment purposes.

Another type of notice is required in a more specific employment setting when there is an adverse action. If a consumer is applying for a position regulated by the Secretary of Transportation or a state transportation agency, and, at the time of the report request, the only contact between the person and the consumer has been by mail, telephone, computer, or other similar means, the person must provide the following information within three business days of taking an adverse action based in whole or in part on a consumer report: that the adverse action has been taken based in whole or in part on a consumer report; the name, address, and telephone number of the consumer reporting agency that furnished the report; a disclaimer that the agency cannot explain why the decision to take the adverse action was made because the agency did not make the decision; and that the consumer can request a free copy of his or her report from that agency and can contest the accuracy and completeness of the report.

Finally, if an adverse action is taken regarding the extension of credit, the underwriting of insurance, or any license or other benefit granted by a governmental entity, and such action is based upon consumer report information that has been furnished by an affiliate, the person must notify the consumer of the adverse action and disclose the nature of the information upon which the action was based if the consumer requests such information in writing within 60 days after notice of the adverse action was sent.

57. What are the Identity Theft Red Flags Rules?

The Identity Theft Red Flags Rules regulations became effective January 1, 2008, and require “financial institutions” and “creditors” who hold “covered accounts” to establish a written program to detect, deter and mitigate identity theft. “Identity theft” is fraud committed or attempted using the identifying information of another person without authority. The final regulations were issued on November 9, 2007, by six federal regulators. The regulations are published separately for each regulator but contain substantially identical provisions. The Red Flags Rules can be found as follows:

- Federal Reserve System (*12 CFR Part 222*)
- Federal Deposit Insurance Corporation (*12 CFR Parts 334 and 364*)
- National Credit Union Administration (*12 CFR Part 717*)
- Federal Trade Commission (*16 CFR Part 681*)
- Department of Treasury's Office of the Comptroller of the Currency (*12 CFR Part 41*)
- Department of Treasury's Office of Thrift Supervision (*12 CFR Part 571*)

58. Who needs to comply with the Identity Theft Red Flags Rules?

The Identity Theft Red Flags Rules regulations apply to “financial institutions,” traditionally regulated by the federal government, as well as others. It also applies to any “creditor,” that is, any business that regularly extends credit, including large and small organizations such as finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, and even small merchants that allow customers to buy on credit. Finally, it applies to entities that provide services to financial institutions and creditors with regard to covered accounts, even though those vendors may not be covered by the Red Flags Rules absent those services. As noted below, the compliance deadline for financial institutions was November 1, 2008; the deadline for compliance by creditors as of the date of these FAQs is currently June 1, 2010.

59. What is considered a “financial institution”?

The definition of “financial institution” is broad and includes state or federal banks, savings and loan associations, credit unions, mutual savings banks, or any persons that (directly or indirectly) hold a “transaction account” belonging to a customer. A transaction account includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

60. Who is considered a “creditor”?

Creditors include (1) any person who regularly extends, renews, or continues credit; (2) any person who regularly arranges for the extension, renewal, or continuation of credit; or (3) any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. The significance of this definition is that a broad cross-section of businesses must comply.

The Red Flags Rules’ definitions of what constitutes “credit” and who is a “creditor” are a little circuitous, but lead to the definition under the Equal Credit Opportunity Act. The regulation defines credit and creditor as:

- Credit has the same meaning as in 15 U.S.C. 1681a(r)(5).
- Creditor has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies.

The Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act (FACTA) (15 U.S.C. 1681a(r)(5)) defines credit and creditor as under the Equal Credit Opportunity Act: “Credit and creditor. The terms ‘credit’ and ‘creditor’ have the same meanings as in section 1691a of this title.”

The Equal Credit Opportunity Act (15 U.S.C. 1691a(d) and (e)) defines “credit” and “creditor” as follows:

- The term “credit” means the right granted by a creditor to a debtor to defer payment of debt, to incur debts and defer payment, or to purchase property or services and defer payment.
- The term “creditor” means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

One key element to being a creditor under this definition is the regularity with which the entity extends, renews or continues credit. If an entity only sporadically offers credit to individuals, then it may not be deemed a creditor under this definition. However, where an entity routinely offers credit for individuals, then it would fall within this definition. It should be noted that the term “credit” encompasses any provision of goods or services with a deferred payment. There is no requirement for multiple transactions or multiple payments under this definition.

61. What type of accounts trigger compliance with the Red Flags Rules?

Covered accounts include (1) any personal accounts designed to permit multiple payments or transactions (e.g., credit card accounts, mortgage or automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts or savings accounts, “house accounts” offered by restaurants); and (2) any other account for which there is a foreseeable risk of identity theft. It is up to each organization to determine the accounts that fall into this category. Business accounts may also be considered covered accounts if there is a history of identity theft, or the risk posed is significant (considering factors such as the number of individuals with access and types of transactions processed).

Two definitions apply to the determination of whether an account is a “covered account.” The regulation defines an “account” as follows:

“Account” means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. “Account” includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account.

Three key elements govern whether an account exists under the Red Flags Rules. First, the relationship must be a “continuing relationship,” meaning not just a onetime transaction. Second, the product or service must be for personal, family, household or business purposes. Third, the term “account” includes an extension of credit to purchase property or services and a deposit account.

Not all accounts qualify for treatment under this regulation, however. The account must be a “covered account” in order to be subject to this rule. The regulation defines “covered account” as follows:

Covered account means:

- An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account,

mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

- Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The critical element here is that the account must “involve” or “be designed to permit” multiple payments or transactions. With the broad wording of the regulation, an account that permits multiple charges but one payment could be a covered account. Similarly, an account with one transaction but multiple payments also would be a covered account.

62. Are the Red Flags Rules limited to consumer accounts?

No. The second part of the definition of a “covered account” refers to “any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” This part of the definition reflects the belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft, and, therefore, should be considered for coverage by the program of a financial institution or creditor.

63. What business accounts are covered?

Any business account that poses a higher risk of identity theft could be a covered account. Primarily, however, it is anticipated that covered business accounts would involve those of small businesses.

64. Do the Red Flags Rules only cover the opening of accounts?

No. The Red Flags Rules apply to covered accounts that are in the process of being opened and those in operation thereafter. As new types of accounts are developed, the covered entity’s “Red Flags Rules Plan” (discussed further in Questions 66 and 67) must be updated to address those accounts as well. The Rules impose obligations when opening accounts and in addressing circumstances that may arise after an account is opened. For example, if a change of address is requested at the same time as a replacement credit card, a “red flag” may be identified and triggered.

65. What is meant by “multiple payments”? Do two installments qualify?

The critical element here is that the account must “involve” or “be designed to permit” multiple payments or transactions. With the broad wording of the regulation, an account that permits multiple charges but one payment could be a covered account. Similarly, an account with one transaction but multiple payments would also be a covered account.

66. Does the Identity Theft Red Flags Rules Plan have to be written?

Yes. The plan must be written, but it can incorporate by reference other existing written plans, policies and procedures that may satisfy some of the requirements of the Red Flags Rules. Examples of such policies and procedures might include a covered entity’s:

- Anti-money laundering (AML) program, particularly those elements related to its customer identification program (CIP), “Know Your Customer” and enhanced due diligence controls, and ongoing suspicious activity monitoring and reporting;
- Customer acceptance procedures;
- Anti-fraud program documentation; and
- Information security program documentation.

67. What does the plan have to include?

The Red Flags Rules require that covered financial institutions and creditors (1) identify relevant “red flags” and incorporate them into their plan, (2) detect “red flags” that are part of the plan, (3) respond appropriately to any “red flags” that are detected, and (4) ensure the plan is updated periodically to address changing risks.

The written plan must provide policies and procedures for dealing with covered accounts and must be approved by the board of directors. Compliance also requires staff training, vendor oversight and periodic updates of the plan. The plan must be dynamic and tailored to the organization's business. It must be able to detect patterns, practices and certain "red flag" activities that could signal possible identity theft.

The plan also needs to identify the types of circumstances that would indicate potential for identity theft (the "red flags") in the opening and operation of the covered account and a means of responding to threats of identity theft if a "red flag" is noted. "Red flags" should be customized to the business and the organization or industry's identity theft experience. A company's history of claims of unauthorized transactions or identity theft by individuals whose identity and credit are used by another without authorization is one source of identifying the "red flags" for identity theft in the covered accounts.

Other sources include industry publications and experiences, and regulatory and other trade publications. The plan is expected to incorporate existing policies and procedures already in place within the organization. Responses to identified "red flags" can run the gamut from declining a transaction, to asking for additional information, to notifying the customer of an issue, to referral to law enforcement, to taking no action.

The Red Flags Rules require that the plan include staff training as necessary to implement the plan effectively. This training may vary by individual roles and the degree of involvement with the plan.

In addition, financial institutions and creditors are expected to maintain appropriate oversight of service providers that perform activities "in connection with one or more covered accounts." Organizations should review applicable contracts to determine if existing provisions require compliance with this type of federal requirement. If not, the contract should be amended so vendor compliance with the Rules is required.

68. Can policies and procedures prepared for compliance with other regulations substitute for the plan?

Written policies and procedures prepared for compliance with other regulations can be included by reference in the Red Flags Rules Plan, but they may not contain, on their own, all the requirements of the Red Flags Rules Plan.

69. We have a Customer Identification Program. Can that be a substitute for the Red Flags Rules Plan?

Under the BSA and its implementing regulations, financial institutions are required to establish programs to verify customers' identities. A CIP established to comply with BSA can be incorporated into the plan, but it might not contain all the requirements of the Red Flags Rules. For example, a CIP may not include service provider oversight or designation of specific "red flags" that are triggered after an account has been opened and is operating.

70. We are Payment Card Industry Data Security Standard-compliant. Is that sufficient?

Portions of the PCI Data Security Standard (PCI DSS) can be incorporated into the Red Flags Rules Plan, but it might not contain all the requirements of the Red Flags Rules. For example, a security breach incident response plan developed for PCI compliance may be incorporated into the Red Flags Rules Plan. However, the Red Flags Rules have additional requirements beyond those required for PCI compliance. Please refer to Question 174 for a description of PCI requirements.

71. Does the plan have to include a list of all the "red flags" we identify?

The plan is expected to be flexible and to address the financial institution's or creditor's business. The Red Flags Rules require a risk assessment from each organization for its accounts, but there is little guidance as to how an organization should ultimately use the results in its determination of which accounts constitute covered accounts. Some "red flags" may be identified that will have a low incidence in the business or will have a low probability of resulting identity theft. The focus of the plan should be on those "red flags" that are good predictors of conduct related to identity theft.

72. Does the plan have to include all the “red flags” in Appendix J of the Red Flags Rules?

No. The circumstances listed in Appendix J of the Red Flags Rules are included as examples of “red flags” and are intended only to provide guidance. The company’s “red flags” will be based on its own covered accounts, its own experiences with identity theft, and the nature of the industry in which it operates. For example, Appendix J lists changes to cellular telephone accounts as a potential “red flag.” Clearly, this would not be applicable to a company that does not offer such services. However, regulatory agency examiners will generally expect, at a minimum, that a covered entity will have considered the applicability of each of the Appendix J red flags to its business, and can evidence the results of this effort using its risk assessment documentation.

73. How do we determine whether a circumstance is a “red flag” for identity theft?

The determination is based on the company’s experience and the risk that the circumstance will or can result in identity theft. “Red flags” should be customized to the business and the organization or industry’s identity theft experience. A company’s history of claims of unauthorized transactions or identity theft by individuals whose identity and credit are used by another without authorization is one source of identifying the “red flags” for identity theft in the covered accounts. Other sources include industry publications and experiences, and regulatory and other trade publications. Appendix J contains a list of examples of red flags, which include notification from a consumer reporting agency, suspicious account documents, suspicious personal identifying information, unusual use of a covered account, or warnings received from customers.

74. What is the deadline for compliance?

Financial institutions subject to the banking agencies’ joint regulation were required to be in compliance by November 1, 2008. The deadline for other covered entities subject to the FTC’s rule has been extended several times; as of the date of this FAQ guide, the latest deadline is June 1, 2010.

75. What are the board of directors’ obligations under the Red Flags Rules?

Under the regulations, the board of directors is tasked with development, approval and enforcement of the plan. Development and enforcement of the plan can be delegated to senior management, but the board, or an appropriate committee of the board, must approve the initial plan and any material amendments. Minor amendments may be implemented without board approval.

The board, or an appropriate committee of the board, must also receive annual reports on the operation of the plan, which should include assessments of the effectiveness of the plan’s policies and procedures, service provider arrangements, significant incidents involving identity theft, and management’s response and recommendations for material plan changes.

76. How often must the plan be updated?

The plan must be reviewed “periodically” and at least annually. This review includes reassessment of the business’s covered accounts and its own and its industry’s experiences with identity theft. When additional “red flags” are identified, either through a periodic review, an annual review or following a security incident, the plan should be updated to reflect the additional or new threats. This may entail reviewing experience with instances of identity theft; changes in methods of identity theft; changes in methods to detect, prevent or mitigate identity theft; changes in the types of accounts offered; or changes in business arrangements.

77. What vendor oversight is required?

A creditor or financial institution is required under the Red Flags Rules to “... ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.” A “service provider” is an entity that provides a service directly to the financial institution or creditor, in particular, those who perform activities in connection with covered accounts.

Each vendor’s activity must be under a compliant Red Flags Rules Plan. The burden is on the creditor or financial institution covered by the regulations to make sure the vendors have a compliant plan.

Financial institutions and creditors have flexibility in terms of how they achieve vendor compliance. For instance, some may impose specific reporting requirements on vendors that perform specific functions with regard to covered accounts. This would include requiring vendors to identify specific “red flags” and report the occurrence or discovery of such a circumstance to the financial institution or creditor who will then take the appropriate steps to respond. Others may choose to allow the vendor to identify the appropriate “red flags” and to develop responses to address them.

78. Do we need to police our vendors?

Vendor oversight, like all aspects of the Red Flags Rules, is intended to be ongoing. Creditors and financial institutions should consider incorporating Red Flags Rules compliance obligations as well as review or audit rights in their contracts with vendors to permit periodic review of the vendor’s compliance with the regulations. As with most other aspects of vendor management, standards for ongoing monitoring of vendor compliance should be risk-based. Vendors that have access to more significant volumes and/or higher-risk types of customer data should be subject to enhanced monitoring controls.

79. Must our vendors adopt our plan?

No. The Red Flags Rules only require that service providers comply with the regulations. Vendors may adopt their own plans or may elect to comply with your plan. When a vendor performs service for multiple financial institutions or creditors, it may be more efficient for the vendor to adopt its own plan. Ultimately, it is the responsibility of the financial institution or creditor to ensure vendor compliance.

80. What due diligence is required when we engage a vendor?

The Red Flags Rules make special note of activities performed “in connection with one or more covered accounts” that are outsourced to third-party service providers. In such instances, the organization has an obligation to ensure that its service providers are compliant with the Red Flags Rules. As part of current implementation efforts, organizations should review all applicable service provider contracts to determine whether existing contract language acknowledges compliance with this type of federal requirement.

81. Do we need to review all vendor contracts before the June 1, 2010 compliance deadline?

Because vendor oversight is part of compliance with the Red Flags Rules, financial institutions and creditors should have reviewed all vendor contracts before the compliance deadline. Organizations should review all applicable service provider contracts to determine whether existing contract language acknowledges compliance with this type of federal requirement or if specific language must be addressed in an amendment.

82. What is the penalty for noncompliance with the Red Flags Rules?

The failure to comply with the Red Flags Rules could result in civil penalties due to certain provisions within the Fair Credit Reporting Act (FCRA). The relevant liability provisions of the FCRA include fines and damages, including punitive damages and attorneys’ fees, for willful noncompliance or for negligent noncompliance with “any requirement imposed” under the FCRA (which now includes the Identity Theft Prevention Program requirement) 15 U.S.C. § 1681n(a), § 1681o.

83. What enforcement mechanisms are in place under the Red Flags Rules?

Any fines or sanctions that arise under the FCRA may only be enforced by the Federal Trade Commission (FTC) or other federal financial regulators. This means that a private right of action in the courts has not been provided for anyone harmed by an organization that fails to comply with the Red Flags Rules.

84. What is the penalty for violating the FCRA?

A person who willfully fails to comply with the FCRA is liable for actual damages or statutory damages between \$100 and \$1,000. A person or a natural person who obtains a credit report under false pretenses, or knowingly without a permissible purpose, is liable for the actual damages sustained or \$1,000, whichever is greater. The court may also award punitive damages and reasonable attorneys’ fees to the party that successfully enforced the FCRA. Additionally, if the court finds that a document was filed in bad faith or for harassment, the court may award attorneys’ fees to the prevailing party for the cost of the improper document.

A person who negligently fails to comply with the FCRA is liable for actual damages and attorneys' fees. Again, if the court finds a document was filed in bad faith or for harassment, the court may award attorneys' fees to the prevailing party for the cost of the improper document.

Knowingly and willfully obtaining information from a consumer reporting agency under false pretenses is punishable by a fine and/or a prison sentence of no more than two years. The same penalty applies to an employee or officer of a consumer reporting agency who knowingly and willfully provides information to an unauthorized person.

The FTC may also enforce violations of the FCRA. A person who knowingly violates the FCRA may be liable for up to \$2,500 per violation, based upon the court's evaluation of the degree of culpability, history of prior such conduct, ability to pay, effect on the ability to continue doing business, and such other matters as justice requires.

In addition to liability to the consumer and to the FTC, those who violate the FCRA can be exposed to states that may bring an action to enjoin the violator from further violations, and to recover damages for residents of the state.

Because the statute carries severe penalties for violation, if you have any question about your compliance with its requirements you should consult your legal professional.

85. What document retention and disposal obligations are imposed by FCRA?

Generally, laws impose document retention obligations based on the purpose of the law. For example, the Age Discrimination in Employment Act and Title VII impose strict document retention obligations to keep track of hiring decisions to protect against discrimination. However, because the FCRA seeks to protect the privacy of consumers, it actually requires the destruction of consumer report information to protect against unauthorized access to or use of that information.

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) directed the FTC, among other governmental entities, to adopt rules regarding the disposal of sensitive consumer report information. Accordingly, the FTC adopted the "Disposal Rule" in 2005, which amended the FCRA by imposing new requirements that any person who maintains or otherwise possesses consumer report information for business purposes must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Accordingly, consumer reporting agencies, lenders, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, attorneys or private investigators, debt collectors, and individuals who obtain a credit report on a prospective nanny, contractor, or tenant, and entities that maintain information from consumer reports for the benefit of any of the aforementioned entities, are subject to the Disposal Rule.

The Disposal Rule is flexible and allows the organizations and individuals subject to it to determine the best disposal measures based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

86. How do users dispose of consumer report information?

As mentioned above, the Disposal Rule is flexible and allows the organizations and individuals subject to it to determine the best disposal measures. However, the FTC lists the following as examples of disposal methods that ensure information cannot be read or reconstructed: burning or shredding papers; destroying or erasing electronic files or media; and conducting due diligence or hiring a document destruction contractor to comply with the Disposal Rule. The FTC provides that due diligence may include: reviewing an independent audit of a disposal company's operations and/or its compliance with the Disposal Rule; obtaining information about the disposal company from several references; requiring that the disposal company be certified by a recognized trade association; or reviewing and evaluating the disposal company's information security policies or procedures.

87. If a company is not a consumer reporting agency, does the FCRA still apply?

The definition of a consumer reporting agency is broad, and, accordingly, a person must determine whether or not it falls within the definition. A "consumer reporting agency" means any entity (person/organization) which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

If an entity clearly does not fall into this broad definition, the FCRA may still apply to the person if the person requests, handles, or uses consumer reports. For example, a person who takes an adverse action based upon a consumer report must comply with certain notice obligations imposed by the FCRA, and users of consumer reports are prohibited from taking certain actions if the credit file contains a fraud alert.

88. What are consumer reporting agencies' obligations to protect or secure consumer report information?

Every consumer reporting agency must maintain reasonable procedures to avoid including prohibited information in consumer reports and to limit the furnishing of consumer reports to the purposes listed under the FCRA. The procedures must require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Each agency must also make a reasonable effort to verify the identity of a new prospective user and the uses certified by such a prospective user prior to furnishing a consumer report. No agency may furnish a consumer report if it has reasonable grounds for believing the report will not be used for a permissible purpose. In addition, the Disposal Rule requires that handlers of consumer reports dispose of sensitive consumer information carefully.

89. Are there limitations on sharing consumer report information? What is the Affiliate Marketing Rule?

Yes, there are limitations on sharing consumer report information. As noted in Question 48, consumer reports are only available in a limited number of circumstances. Further, information that ordinarily would be considered consumer report information is taken outside that definition in specific instances, such as when experiential information is shared with affiliates.

As of October 1, 2008, the Affiliate Marketing Rule took full effect. The rule limits the *use* of shared consumer report information. The Affiliate Marketing Rule was promulgated by the FTC under the FCRA and can be found at 16 CFR parts 680 and 698. Under the rule, affiliates may not use consumer report information received from an affiliated company to make a solicitation for marketing purposes, unless the consumer has been notified that the information may be used by affiliates for marketing purposes, and the consumer is given the opportunity to opt out in a simple way. This means, for instance, that transactional information (which when shared with an affiliate falls into an exception from the definition of consumer report information) can be received by the affiliate under the FCRA, but cannot be used by that affiliate for marketing purposes without disclosure and an opt-out being provided.

90. What must be included in an affiliate marketing disclosure?

The disclosure must be clear and conspicuous and must allow the consumer to prohibit all solicitations; however, the opt-out may allow the consumer to choose from different options, including the types of entities and information covered by the opt-out, and which methods of delivery the consumer wants to prohibit. If a consumer chooses to opt out, the prohibition must be effective for at least five years, unless revoked earlier by the consumer. At the end of the five-year period, the consumer must be given a clear and simple way to extend the opt-out for another period of at least five years. For the purposes of affiliate sharing, "solicitation" means the marketing of a product or service initiated by a person to a particular consumer that is based on an exchange of information, and intended to encourage the consumer to purchase the product or service, but does not include communications directed at the general public.

The foregoing restrictions do not apply when: (1) the person seeking to use the shared information has a pre-existing business relationship with the consumer; (2) the shared information is used to assist in communications with an individual who receives employee benefits or services pursuant to a contract with his or her employer, relating to that person's status as a participant or beneficiary of an employee benefit plan; (3) the shared information is used to perform services on behalf of another affiliate, provided the other affiliate would have itself been permitted to send the solicitation; (4) the shared information is used in response to a communication initiated by the consumer or in response to solicitations authorized or requested by the consumer; and (5) when compliance with these restrictions would prevent compliance with state insurance laws prohibiting unfair discrimination. A "pre-existing business relationship" with the consumer is a relationship based on an existing financial contract; the consumer's purchase, rental, or lease of goods or services; a financial transaction that occurred within the 18 months prior to the solicitation; or a solicitation by the consumer within the three months preceding the solicitation.

The Affiliate Marketing Rule restrictions apply to consumer report information without regard to the exemptions for experiential or transactional information (see Question 89). Thus, while *sharing* of transactional information among affiliates is permitted without making the entity sharing the information a consumer reporting agency, and without violating the FCRA, *using* the information by the affiliate for direct marketing is prohibited unless the disclosure and opportunity to opt out is provided.

91. What is an “affiliate”?

An “affiliate” is a person related by common ownership or affiliated by common corporate control to the person taking the action.

92. What information is considered “experiential”?

Experiential, or transactional, information is data regarding only the transactions between the person making the report and the consumer. This type of information is not considered consumer report information, and disclosure is not prohibited under the FCRA.

Children’s Online Privacy Protection Act (COPPA)

93. What is the Children’s Online Privacy Protection Act?

The 1998 Children’s Online Privacy Protection Act (COPPA) regulates the online collection of personal information from children under the age of 13. The goal of COPPA is to give parents more control over the collection and use of such information. COPPA, in conjunction with the Children’s Online Privacy Protection Rule (Rule) promulgated by the Federal Trade Commission (FTC) in 1999, dictates what content website operators must include in their privacy policies, when and how to obtain parental consent to collection, and what an operator must do to protect children’s information.

94. To whom does COPPA apply?

COPPA applies to any operator of a commercial website or online service that collects personal information from children under the age of 13. “Personal information” includes a child’s first and last name, home or other address, e-mail address, telephone number, Social Security number, other identifiers that would allow someone to contact an individual child, or information about a child or a child’s parents in combination with any previously listed information.

The FTC is responsible for making individualized determinations of whether an entity is an “operator” for the purposes of COPPA. To make such a determination, the FTC considers whether the entity in question owns and controls the information collected, whether it pays for the collection and maintenance of the information, what pre-existing contractual relationships there are in connection with the information, and what role the website plays in collecting or maintaining the information. In the event more than one operator exists for a site or service, all will be jointly responsible for compliance.

It is important to recognize that an entity may be subject to COPPA even if its website or service is not specifically directed to children. For example, general audience websites that have a separate area for children must also comply. Additionally, compliance is required if the operator has actual knowledge that its general audience website is collecting personal information from children under the age of 13. See Questions 99 and 102 for more information on this topic.

95. What information may website operators collect from a child without first obtaining parental consent?

Under COPPA, an operator of a website may collect the name and online contact information of a child, such as an e-mail address, without prior parental consent in five circumstances:

- First, an operator may request this information, or the online contact information of a parent, in order to obtain parental consent to maintain a child’s information. If an operator does not affirmatively receive parental consent (i.e., if the parent refuses or if the parent does not respond), then it must delete the child’s contact information.

- Second, an operator may collect this information if it is used solely and directly to respond to a onetime, specific request from that child. For example, an operator may e-mail a child in response to a brief question about the website's features or a specific promotion. After fulfilling the request, the operator may not re-contact the child and the child's personal information must be deleted.
- Third, an operator may collect this information for continued response to a specific request, but the operator may not contact the child beyond the scope of the request. This exception might apply, for example, where an operator wishes to collect a child's e-mail address for the sole purpose of providing password reminders to that child. However, an operator must make reasonable efforts after the initial response to provide a parent with notice of the information that it has been collecting from the child, and give the parent the opportunity to request that the information not be used.
- Fourth, an operator may use this information to the extent necessary to protect the safety of a child visiting its website. The information may only be used to protect the child's safety, and it may not be used to re-contact the child for any other purpose. Again, the operator must make reasonable efforts to provide a parent with notice of the information collected, and give the parent the opportunity to request that the information not be used.
- Finally, an operator may collect a child's name and online contact information to the extent necessary to protect the security or integrity of a website, take precautions against liability, respond to judicial process, or provide information to law enforcement agencies or for investigations on matters related to public safety (as permitted by other laws).

96. How do operators verify that a parent has consented?

An operator may verify consent by any method that reasonably ensures that the person providing consent is the child's parent. The appropriateness of a method for meeting this goal depends upon how the operator intends to use the child's information.

If an operator intends to disclose a child's information to a third party, the operator might (1) require a form to be signed and returned by mail or fax, (2) require a parent to use a credit card to conduct a transaction (such as a membership fee, purchase, or nominal fee for processing the credit card) and verify the credit card number, (3) allow parents to call a toll-free number staffed by trained personnel, or (4) obtain e-mail consent with a digital signature or other digital certificate. These methods are also advised if an operator intends to make the information publicly available via social networking sites, blog services, personal home pages, chat rooms, e-mail accounts, etc.

If an operator only intends to use a child's information for internal purposes, such as marketing to the child or communicating promotions, the operator has more options for verification. It may use any of the above methods, or (1) obtain e-mail consent followed by a letter or phone call to the parent, or (2) send a delayed confirmatory e-mail to the parent, with notification and the opportunity to revoke consent.

97. What security procedures must operators have in place when they hold children's information?

The rule requires an operator to use reasonable procedures to protect the confidentiality, security, and integrity of children's information. This includes protecting information against loss, misuse, and unauthorized access or disclosure. "Reasonable procedures" may include, but are not limited to, using firewalls, deleting personal information no longer in use, training employees in data handling and limiting their access to information, and screening third parties before disclosing any information to them.

98. What verification should operators require for someone to access the child's information?

Before granting a third party access to a child's information, an operator must give the parent an opportunity to object to third-party disclosure. This rule does not apply if an operator discloses information to a third party solely in support of the internal operations of the website (e.g., technical support, order fulfillment). But if a subsidiary intends to use the information in other ways, then the operator must seek consent and notify the parent whether the subsidiary is bound by the website's privacy policy.

99. How does one determine whether a website "attracts" children?

COPPA sets out a number of factors that the FTC uses to determine whether a website is directed to, or attracts, children. These factors include the subject matter of a website, its visual and/or audio content, the age of the models on the website,

the type of language used on the website, and whether advertising on the site is directed to children. For example, use of brightly colored and/or simplistic or animated characters is a typical indicator that a website is designed to attract children. The FTC may also consider evidence regarding the actual and intended age of a website's users to determine whether a site attracts children.

100. An operator wants to offer birthday coupons to children. Does it have to comply with COPPA?

An operator who offers birthday coupons to children under 13 needs to comply with COPPA. The FTC has previously initiated enforcement actions against companies that have offered birthday promotions to children under the age of 13 where such programs required children to list their names, addresses, birthdays, and other information, and did not give parents the opportunity to review or delete the information.

101. What do operators need to do to verify the child's age?

An operator who maintains a general audience website is not required to verify a child's age or to comply with COPPA unless it has actual knowledge that its website is collecting information from children under the age of 13. If an operator has actual knowledge that its general audience website collects information from children under age 13, or if it wishes to collect demographic data including age for other reasons, then the operator should use collection methods that do not encourage children to falsify their age.

For example, an operator might ask for age information when it asks users to provide personal information or create a login user ID, but should not notify users in advance that they can only continue if they are over age 12. In addition, an operator should collect age information in a neutral manner. This may mean asking users to enter their full date of birth, rather than providing users with a drop down box that begins at age 13 or asking users to check a box certifying that they are over 12 years old. Operators may also want to use a cookie to prevent a user from going back to enter a different age.

102. What should an operator do if it suspects children are using its site and providing information?

Once an operator verifies that children are using its website, it has several options.

First, an operator may collect parents' addresses to give them notice and obtain consent under COPPA. If an operator does not wish to obtain parental consent, it may cease collecting personal information from children and delete the previously collected information, instead redirecting children to portions of the website that do not collect personal information and configuring its website to automatically delete any information collected from children.

An operator might also consider whether it falls under one of the e-mail exceptions to prior consent, how it can use screen names or other anonymous identifiers to personalize the website, and how it might limit the amount of information collected from children. These options often allow operators to continue to offer content to children, without violating COPPA.

Finally, an operator may choose to block children from its website. After verifying a child's age, an operator may notify the child that he or she cannot register at this time, and if possible use a cookie to prevent back-clicking. If an operator chooses to block children from its website, it is important that the website does not encourage children to falsify their age.

103. Can website operators market to children over the age of 13?

A website operator may market to children over age 13, but should be aware that a website directed at teenagers might still attract many children under the age of 13. Thus, the website operator may want to take precautions to verify the child's age. The FTC also encourages operators, notwithstanding COPPA, to establish privacy protections for teenagers. Some states have legislation restricting marketing to children, such as California's Penal Code Section 637.9 prohibiting the use of information collected from a child under the age of 16 in a commercial setting for marketing to that child or its family if the parent or legal guardian objects, Child Registry statutes in Utah and Michigan prohibiting certain marketing to registered children under the age of 18, and Maine's statute prohibiting certain marketing to children under 18.

104. Does COPPA apply to off-line information collection?

COPPA does not apply to requests and collection of information off-line. However, COPPA defines “Internet” broadly. According to COPPA, the term “Internet” means, collectively, the myriad computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP), or any predecessor or successor protocols to such protocol, to communicate information of all types by wire or radio. Therefore, COPPA does apply to the collection of information by any computer or telecommunications network that uses TCP/IP or similar protocols to transmit information, which may include Voice over Internet Protocol (VoIP) systems.

105. Do pictures of children constitute “information”?

A photograph of a child constitutes “information” when associated with other information collected online that would allow someone to identify and contact that child. An operator is therefore subject to COPPA when it seeks photos of children in conjunction with names, addresses, e-mail addresses, phone numbers, or any other information that would enable someone to contact a child.

106. What are the penalties for violating the statute?

Website operators may be liable for civil penalties of up to US\$11,000 for each individual violation of COPPA. When assessing penalties, a court may look at the egregiousness of the violation, the number of children involved, the volume and type of information collected, how the information was used, and the size of the website operator.

107. Are there other laws or regulations that limit marketing to children?

Yes. There are a number of state statutes that limit the collection and use of information in marketing to children. Some examples are the Utah and Michigan Child Registry Statutes, the Maine Predatory Marketing to Minors Statute (which all apply to children under the age of 18) and California’s Penal Code Section 637.9 (which applies to children under the age of 16). At this point, the Maine Predatory Marketing to Minors Statute is under review by the Maine legislature and may be significantly amended or repealed. However, it serves as a good example of the thinking of state legislatures in this area as other states have and continue to consider means of protecting children from marketing through legislation.

Right to Financial Privacy Act (RFPA)

108. What is the Right to Financial Privacy Act?

The Right to Financial Privacy Act (RFPA) of 1978 is a federal law that seeks to protect records and other information regarding individuals’ financial activities. The RFPA was enacted to codify the rights of financial institution customers to expect that their financial activities have a reasonable amount of privacy from federal government scrutiny. The RFPA establishes specific procedures for government authorities that seek information from a financial institution about a customer’s financial records and imposes limitations and duties on financial institutions prior to the release of information sought by government agencies. Liability and penalties can be imposed on both government agencies and financial institutions for violating the requirements of the RFPA.

Prior to the RFPA, customers could not challenge government access to their financial records. Nor did customers have any way of knowing that their personal records were being turned over to a government authority. In 1976, the U.S. Supreme Court held in *United States v. Miller* (425 U.S. 435 (1976)) that financial records, because they are kept by the institution, are the property of the institution rather than the customer. As such, the customer had no protectable legal interest in the records kept by the financial institution, nor could he or she limit government access to those accounts. The RFPA was passed principally in response to this U.S. Supreme Court decision.

The RFPA generally requires that the customer must receive the following: written notice of the governmental agency’s intent to obtain financial records; an explanation of the purpose for which the records are sought; and a statement describing the procedures to use if the customer does not wish such records or information to be made available. There are certain exceptions in the RFPA that may apply to allow for delayed notice or no notice to be given to the customer.

109. Who is covered by the RFPFA?

The RFPFA applies to financial institutions, government authorities and customers of financial institutions. A “government authority” refers to any agency or department of the United States, or any officer, employee, or agent thereof. A “customer” refers to any person or authorized representative of that person who uses or has used any service of a financial institution, and includes any person for whom that financial institution acts or has acted as a fiduciary in relation to an account maintained in that person’s name. (Please refer to Question 110 below for the definition of “financial institution.”)

110. What is a “financial institution” for purposes of the RFPFA?

The RFPFA defines a “financial institution” as any office of a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan association, homestead association (including cooperative banks), credit union, or consumer finance institution.

The term “card issuer” means any entity who issues a credit card, or the agent of the entity with respect to such card. The term “credit card” means any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit. Under current definitions, a “card issuer” generally refers to any entity that issues a credit card. Traditional bank credit card issuers are covered by the term “card issuer,” but the definition also includes retailers and other merchants (such as gasoline companies) that issue their own credit cards (even though such entities are not usually thought of as “financial institutions” in the traditional sense).

The definition of “financial institution” was expanded beginning in July 2002, and now includes, in addition to depository institutions (e.g., banks, thrifts and credit unions), many entities that most individuals would not consider traditional financial institutions, such as: money services businesses; money order issuers, sellers and redeemers; traveler’s check issuers, sellers and redeemers; the U.S. Postal Service; securities and futures industries; futures commission merchants; commodity trading advisors; and casino and card clubs. There is a point of current confusion in the law regarding whether the definition of “financial institution” includes issuers of travel and entertainment cards that do not permit customers to defer payment; case law has yielded mixed results on this question.

The RFPFA covers financial institutions located in any state or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa or the Virgin Islands.

111. Do the protections under the RFPFA extend to all of an institution’s customers, or only to individuals?

RFPFA protections extend only to an individual or a partnership of five or fewer individuals.

112. Upon receipt of a government agency request for financial records, does an institution need to notify its customer?

No. Under the RFPFA, the financial institution has no obligation to notify the customer that a government request for information has been made, although there may be circumstances in which the financial institution has notification obligations outside of the RFPFA. The government authority making such a request is generally responsible for providing the customer with the appropriate notice as required by the RFPFA. In some cases, customer notification may be delayed if the government authority makes an application to a presiding judge or magistrate judge and such presiding judge or magistrate judge finds: (1) that the investigation being conducted is within the lawful jurisdiction of the government authority seeking the financial records; (2) there is reason to believe that the records being sought are relevant to a legitimate law enforcement inquiry; and (3) there is reason to believe that such notice will endanger the life or safety of any person, induce flight from prosecution, result in destruction of or tampering with evidence, result in intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or official proceeding or unduly delay a trial or other official proceeding.

113. Are any records excluded from the RFPFA?

The RFPFA provides a number of exceptions under which the consumer protections generally afforded by RFPFA do not apply. These exceptions are allowed generally because the customer’s rights are already protected by other legal

procedures or because the disclosures are not aimed at a particular individual. In these situations, disclosure by a financial institution is always permitted, and no authorization, subpoena, or warrant is required. Some of the exceptions under which financial institutions can disclose customer records, as listed in the RFPA, are as follows:

- Disclosures of records that do not individually identify a particular customer.
- Disclosures in the financial institution's interest, including perfection of security interests, government loans, loan guaranties and loan insurance; proving a claim in bankruptcy; and collecting a debt for itself or a fiduciary.
- Disclosure to, or examination by, a supervisory agency pursuant to exercise of supervisory, regulatory or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties or other persons (including regular examinations and consumer complaints).
- Disclosures sought in accordance with procedures authorized by the Internal Revenue Code, which has its own individual privacy protections.
- Disclosures pursuant to other federal statutes or rules, administrative or judicial proceedings.
- Disclosures that are relevant to possible violations of the law (Suspicious Activity Reports). Such disclosures to law enforcement are generally limited to the name of the account holder and the nature of any suspected illegal activity.
- Emergency disclosures and disclosures to federal agencies charged with foreign intelligence, counterintelligence, or other national security protective functions.

114. What are an institution's reporting obligations under the RFPA?

Upon receipt of a government agency request for financial records, a financial institution is obligated to begin assembling the requested records and must be prepared to deliver the records to the government agency upon receipt of a written certificate of compliance. The financial institution must maintain a record (e.g., date, name of the government authority, and an identification of the records disclosed) of the disclosure to the government agency pursuant to customer authority. A financial institution may not release a customer's financial records until the government authority seeking them certifies in writing that it has complied with the RFPA.

To obtain access to, copies of, or information contained in a customer's financial records, the requesting government authority generally must present to the financial institution one of the following certificates:

- A customer authorization (for a period not to exceed three months), signed and dated by the customer, that identifies the records, the reasons why the records are being requested, the customer's rights under the RFPA, and states that the customer may revoke the authorization at any time before disclosure.
- An administrative subpoena or summons.
- A search warrant.
- A judicial subpoena.
- A formal written request by a government agency (only if no administrative summons or subpoena authority is available).

115. Are there regulations that govern or relate to the RFPA?

Yes. Federal government agencies frequently incorporate or reference the RFPA in their respective regulations. Many federal regulations also govern the authorization of departmental units to request financial information from a financial institution under the RFPA.

Federal regulations addressing the RFPA include those governing the Federal Reserve System, the Federal Deposit Insurance Corporation, the Department of the Treasury, the National Credit Union Administration, the Federal Trade Commission, the Commodity Futures Trading Commission, the Securities and Exchange Commission, the Department of Justice, the Office of the Secretary of Labor, the Office of the Secretary of the Treasury, the Office of the Secretary of Defense, the Department of the Army, the Department of Veterans Affairs, the U.S. Postal Service, and the Department of Health and Human Services.

116. Are there similar statutes at the state level?

Yes. The RFPA applies to requests for customer financial information made only by federal government entities and does not apply to requests for orders for information by state and local government entities. However, many states have enacted customer protection laws that provide virtually the same protection as that given to customer financial records under the RFPA, and these state laws are applicable to that state's state and local governmental entities. As of May 2009, these states include Alabama, Alaska, Connecticut, Illinois, Louisiana, Maine, Maryland, New Hampshire, North Carolina, North Dakota, Oklahoma, Oregon, Utah, and Vermont.

Other states provide other forms of customer protection. For example, Florida and Massachusetts provide additional customer protections for financial electronic transfer systems. Minnesota requires quarterly disclosure of all account information to the local government regarding any noncustodial parent owing child support. California entitles bank customers to a ten (10) day notice before a state investigator can obtain the customer's financial records.

117. What is the penalty for violating the RFPA?

A financial institution that discloses financial records or information contained therein in violation of the RFPA can be held liable (along with any federal government agency or department obtaining the information in violation of RFPA) to the customer to whom the records relate in an amount equal to the sum of:

- \$100 without regard to the volume of records involved;
- Any actual damages sustained by the customer as a result of the disclosure;
- Such punitive damages as the court may allow, where the violation is found to have been willful or intentional; and
- In the case of any successful action to enforce liability under the RFPA, the costs of the action together with reasonable attorneys' fees as determined by the court.

A financial institution has a good faith defense, however, if the financial institution or one of its agents or employees discloses customer financial records in good faith reliance upon a certificate by any government authority. In such a case, the financial institution will not be liable to the customer for such disclosure.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)

118. What is CAN-SPAM?

CAN-SPAM is an acronym that stands for the Controlling the Assault of Non-Solicited Pornography and Marketing Act. This federal law, which became effective January 1, 2004, establishes (1) guidelines for those who send certain types of "commercial e-mail," (2) penalties for illegally sending such "commercial e-mail" or knowingly benefiting from illegal "commercial e-mail," and (3) methods for consumers to stop unwanted "commercial e-mail." CAN-SPAM was enacted as a response to state e-mail laws that were more restrictive than the federal government's spam rules. Under CAN-SPAM, unsolicited e-mails are not altogether prohibited; however, the Federal Trade Commission has been granted increased authority to stop spam.

119. What communications are covered by CAN-SPAM?

CAN-SPAM applies to two categories of e-mail and also to Internet-based messages sent to wireless mobile devices. The two categories of e-mail subject to CAN-SPAM are "commercial messages" and "transactional or relationship messages." Commercial e-mails include messages with the primary purpose of advertisement or promotion of a commercial product or service. E-mails fall within this category when they:

- Contain exclusively advertising or promotional information;
- Consist partly of advertising or promotional information, but the subject line of the e-mail focuses on the commercial message;

- Consist partly of advertising or promotional information, but the noncommercial content does not appear at the beginning of the body of the message; or
- Consist partly of advertising or promotional information, but a reasonable reader would conclude that the purpose of the message is to promote goods or services.

Transactional or relationship e-mails communicate with existing customers about previously purchased goods or services. E-mails fall within this category when they:

- Facilitate or confirm a commercial transaction that the recipient has already agreed to;
- Provide safety or warranty information about a product or service that the recipient uses or has purchased;
- Notify members, subscribers, or comparable ongoing customers of changes in the terms and features of a product or service;
- Notify ongoing customers of changes in the recipient's status;
- Provide periodic reports on account balance or other account information;
- Inform the recipient of product updates or upgrades that come with a purchase that the recipient previously agreed to; or
- Explain employee benefits in which the recipient is currently participating.

Additionally, CAN-SPAM addresses Internet-based messages to mobile wireless devices. This means that when a sender uses a short message service (SMS) or similar method to transmit commercial messages over the Internet from a computer to a mobile phone or other wireless device (such as a BlackBerry), those messages must comport with CAN-SPAM.

120. Does CAN-SPAM apply to business-to-business communications, as well as communications to consumers?

Yes. The definition of "commercial e-mail" does not distinguish whether the recipient is a business or a consumer. If an e-mail meets the definition, it is covered by the law.

121. What are the requirements for compliant e-mails?

To comply with CAN-SPAM, commercial e-mails must follow certain guidelines to prevent consumer confusion and deception regarding the purpose of the message. Although the requirements differ for transactional or relationship e-mails and for messages to wireless devices, they too are designed to stop customer deception.

A commercial e-mail must:

- Clearly and conspicuously identify the message as an advertisement;
- Include the sender's valid physical address;
- Identify the source of the message in the header information (the header must not contain false or misleading information);
- Not have a deceptive subject line; and
- Provide an opt-out method for recipients to stop future messages. This may take the form of a return e-mail address or another Internet-based response mechanism.

A transactional or relationship e-mail may not contain false or misleading header information, but it is not required to provide the same disclosures as commercial e-mails regarding the nature of the message.

To send a message to a wireless device (a "mobile service commercial message" or MSCM), the sender must obtain "express prior authorization, either orally or in writing," and disclose to the recipient that:

- The recipient is agreeing to receive MSCMs sent to the recipient's wireless device by a particular sender (i.e., blanket authorizations do not work);
- That the subscriber may be charged by the subscriber's wireless service provider for receiving the MSCMs; and
- That the recipient may revoke his/her authorization at any time.

Even with the recipient's advance consent, MSCMs must comply with the rules for commercial e-mails provided above, including providing a valid opt-out method.

122. Does CAN-SPAM prohibit broad e-mail “blasts”?

E-mail “blasts” and distribution of marketing messages in bulk are not expressly prohibited under CAN-SPAM. The number of commercial e-mails a sender distributes is not as significant as the content of the messages and the method used to acquire the e-mail addresses. However, e-mail “blasters” should be aware that additional penalties are imposed on those who engage in “aggravated violations,” which include:

- “Harvesting” e-mail addresses, or taking e-mail addresses from websites or web services that have published a notice against transferring the addresses for solicitation;
- “Dictionary attacks,” or generating e-mail addresses by randomly combining names, letters, and numbers;
- Using scripts or other automated means of registering for multiple e-mail/user accounts;
- Relaying e-mails through another’s computer or network without permission.

123. Can senders e-mail existing customers without restriction?

There are some limitations on messages that can be sent to existing customers by e-mail. A message will be considered a commercial e-mail, even if the sender has done business with the recipient before, if the primary purpose of the message is not to provide updates but to promote the purchase of products or services. A transactional or relationship message, which facilitates or completes an agreed-to transaction with a customer, can be sent without restrictions. However, such transactional and relationship messages may not contain false or misleading header information.

124. Are only advertising e-mails covered by CAN-SPAM?

Advertising e-mails are the primary focus of CAN-SPAM, but transactional and relationship e-mails are also covered under this law if their purpose is to promote a product or service. The Federal Trade Commission explains that CAN-SPAM “covers e-mail whose primary purpose is advertising or promoting a commercial product or service, including content on a website.”

125. What are senders’ obligations to provide “opt-outs”?

Commercial e-mails must provide an “opt-out” function that allows recipients the ability to stop future messages. Either a return e-mail address or an Internet-based form should be used to facilitate opting out. If senders use an Internet-based form, they may give recipients the option to continue receiving specific types of e-mails, as long as the recipient can still choose to stop receiving all messages.

Senders of commercial e-mail must make every effort to honor opt-out requests. The recipient must be able to exercise the opt-out function for at least thirty (30) days after receiving the message. When a sender of commercial e-mail receives an opt-out request, the request must be honored within ten (10) business days. Finally, it is illegal for a sender of commercial e-mail to sell or transfer the e-mail address of a recipient who has submitted an opt-out notice.

126. A company has an e-mail newsletter service for customers. Can it add customers without their consent?

Newsletters are categorized as transactional or relationship e-mails if they provide only information, or if the newsletter provides both information and commercial content. However, e-mail catalogs or other periodic messages with pure commercial content are considered commercial e-mails, and, thus, must provide an opt-out opportunity and honor opt-out requests.

127. Can senders sell their customers’ e-mail addresses?

Under CAN-SPAM, once a recipient has opted out of receiving commercial e-mails, it is illegal for the sender, or anyone else who is aware of the opt-out, to sell or exchange that e-mail address.

If a recipient has not opted out of receiving commercial e-mails, then a company must consider the circumstance under which it received the e-mail addresses to determine the legality of selling those addresses. If a company agrees not to

sell customer addresses or posts a privacy policy promising not to sell e-mail addresses, then the company could face penalties under the Federal Trade Commission (FTC) Act for unfair or deceptive business practices for breaching its agreement with its customers.

The FTC suggests the following to spam-conscious consumers: “Check the privacy policy when you submit your address to a website. See if it allows the company to sell your address. You may want to opt out of this provision, if possible, or not submit your address at all to websites that won’t protect it.”

128. What is the penalty for violating CAN-SPAM?

Those who violate CAN-SPAM could face lawsuits from states, Internet service providers (ISPs), and the FTC. States can sue violators for up to \$250 per violation with a cap of US\$2 million per incident. ISPs can sue and recover up to \$100 per e-mail for false or misleading transmission information and \$25 per e-mail for other violations, up to US\$1 million per incident. The courts can award a state or ISP up to three times the cap amount in cases where the defendant sender willfully and knowingly violated the Act or committed an aggravated violation (such as address harvesting, dictionary attacks, relaying messages by unauthorized access to another’s computer, or creating e-mail addresses through automated scripts).

The FTC can also enforce penalties against anyone who violates CAN-SPAM. Potential penalties from the FTC aim to provide restitution and may include taking any profits from illegal e-mails or stopping senders from continuing business.

Additionally, senders violating CAN-SPAM could potentially face criminal charges. Fines, or even imprisonment of up to five years, may be imposed if a defendant is a repeat offender or has sent multiple commercial e-mails in furtherance of a felony and also (1) accessed a computer without authorization; (2) used relays or retransmitting to deceive the recipient; (3) included false header information; (4) registered two or more domain names or five or more e-mail accounts with false information; or (5) falsely represented themselves as owners of several Internet protocol addresses.

129. Who is at risk if there is a violation?

If there is a violation of CAN-SPAM, the “sender” of the message is at risk for liability. CAN-SPAM defines the sender generally as “a person who initiates ... a message and whose product, service, or Internet website is advertised or promoted by the message.” If someone creates the message and sends it, or if someone procures the creation and delivery of the message, he or she is considered a “sender” under CAN-SPAM. The statute anticipates that there may be multiple parties that qualify as “senders” of a single e-mail, including the advertiser, the person sending the initial e-mail, and any person resending or forwarding the e-mail.

Additionally, a business can be deemed a sender when the business holds itself out as one single entity, even if the message came from a specific division of the company. Third parties also can be held liable for the actions of others under CAN-SPAM. If a business (1) knew or should have known that its goods or services were being promoted through illegal commercial e-mails; (2) benefited economically from e-mails that violate CAN-SPAM; and (3) took no reasonable action to prevent, detect, or report the transmission of the e-mails, then the business may also be held liable.

130. Is there a “Do Not E-mail” registry?

Currently, a nationwide marketing “Do Not E-mail” registry has not been established. Congress has contemplated creating such a registry, which would be analogous to the National Do Not Call Registry, and even requested a report on the viability of a registry. However, the idea was rejected by policymakers who realized that creating such a publicly available list could actually increase spam, especially from outside of the United States.

131. Are there similar laws on the state level that one needs to be aware of?

CAN-SPAM pre-empts any previously existing state laws that deal specifically with using electronic mail to send commercial messages. However, state laws may still apply if they:

- Prohibit falsity or deception in any part of a commercial e-mail or attachment;
- Apply to trespass, contract, or tort law (not specifically to e-mail); or
- Address fraud or computer crime.

Electronic Communications Privacy Act (ECPA)

132. What is the Electronic Communications Privacy Act?

The Electronic Communications Privacy Act (ECPA) is a federal law regulating the interception, disclosure, and storage of wire and electronic communications. The purpose of the ECPA is to protect the privacy of individuals and provide remedies for violations of this law. The ECPA was passed in 1986 to extend existing rules about wiretapping to new forms of communication, such as e-mail. Since then, it has been amended on several occasions, and some states have imposed stricter rules about electronic communications by passing their own laws.

The ECPA has three parts, which are known as titles. Title I (the Wiretap Act) limits the interception, disclosure, and use of wire, oral, and electronic communications during transmission and is codified at 18 U.S.C. §§ 2510-22; Title II (the Stored Communications Act) limits access to stored electronic communications and is codified at 18 U.S.C. §§ 2701-11; and Title III (the Pen Register Statute) addresses the use of devices that record data about phone calls, but not the content of the calls themselves, and is codified at 18 U.S.C. §§ 3121-27.

133. Who needs to comply with the ECPA?

Title I of the ECPA applies to any “person” who intentionally intercepts or attempts to intercept any wire, oral, or electronic communications, or who intentionally discloses or uses or attempts to disclose or use illegally intercepted communications. The term “person” means any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

Title II of the ECPA broadly applies to “whoever” obtains, alters, or prevents authorized access to stored wire or electronic communications without the proper authorization. Additional requirements apply to “a person or entity” who/that provides “electronic communication service” or “remote computing service” to the public. The term “person” is defined as above, and “entity” is not defined. “Electronic communication service” means any service that provides users the ability to send or receive wire or electronic communications. “Remote computing service” refers to the provision to the public of computer storage or processing services by means of an electronic communications system. An “electronic communications system” is any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Title III of the ECPA applies to any “person” who installs or uses pen registers or trap and trace devices without a court order, but does not define “person.” However, providers of electronic or wire communication services, as defined above, face slightly different rules. They are allowed to use such devices to maintain or protect their service and its users from unlawful or abusive use of service, or when the user consents to the device.

134. Are ISPs covered?

Yes. Internet service providers (ISPs) that are considered an individual, partnership, association, joint stock company, trust, or corporation must follow the requirements imposed by the ECPA on any “person.”

Additional rules apply to entities that provide electronic communication service or remote computing service to the public, which, based on the definitions of “electronic communication service” and “remote computing service,” likely include ISPs. Such providers are prohibited from intentionally disclosing the contents of wire and electronic communications transmitted, stored, carried, or maintained by the service to any person or entity other than the addressee or intended recipient of such communications. However, such communications may be disclosed in limited circumstances, including with the lawful consent of the originator or any addressee or intended recipient, to a person employed or authorized, or whose facilities are used, to forward such communications to their destination, or if the communications were inadvertently obtained and appear to pertain to the commission of a crime (provided that such disclosure is made to a law enforcement agency). Such exclusions are discussed in more detail in Question 135.

135. What privacy obligations are imposed by the ECPA?

The ECPA mandates that wire, oral, or electronic communications not be intercepted, disclosed, or used, or that stored communications not be accessed except under certain limited circumstances, which include when necessary to investigate crime or terrorism, when necessary for providers to maintain and protect their services from abusive or unlawful use

of service, and when the communication was not sufficiently private to deserve protection (e.g., oral communications between a police officer and prisoner, or transmissions on citizens' band radio systems). Such limited circumstances are discussed in more detail in Questions 136 and 137.

Even when communications may lawfully be intercepted or accessed, the ECPA includes privacy protections. For example, court orders allowing interception must be written to limit the chances of collecting more communications than necessary for an investigation, and under certain circumstances, subscribers or customers must receive notice before their stored communications are disclosed.

“Wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce, and such term includes any electronic storage of such communication.

“Oral communication” only includes utterances made by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation. “Electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate or foreign commerce, with the exception of wire or oral communications, communications from tone-only pagers and tracking devices, and certain types of electronic funds transfer information.

136. What security obligations are imposed by the ECPA?

The ECPA requires providers of wire and electronic communication services under certain circumstances to intercept wire and electronic communications during transmission or access stored communications, and provide such information to the appropriate governmental entity when necessary to investigate crime or terrorism. Governmental entities can compel providers to supply this information through a variety of methods, including court orders, warrants, subpoenas, and certifications from the attorney general's office. Providers are then prohibited from disclosing to any person that communications have been sought or obtained by the government. The ECPA also permits the disclosure of communications to law enforcement agencies if such communications were inadvertently obtained, and if the communications appear to pertain to the commission of a crime.

137. What are the protections required for stored communications?

The ECPA protects stored communications by imposing penalties on anyone who obtains, alters, or blocks access to stored wire or electronic communications by accessing electronic communication service facilities without the proper authorization. Such penalties are discussed in Question 139.

The ECPA also prohibits providers of electronic communication or remote computing services to the public from disclosing the content of stored communications to any person besides the addressee or intended recipient of such communication, except:

- When requested by a governmental entity by a warrant;
- With the lawful consent of the originator or an addressee, or the subscriber in the case of remote computing service;
- To a person employed or authorized or whose facilities are used to forward the communication to its destination;
- In order to properly provide services or protect the provider's rights or property;
- To law enforcement agencies, if the communication was inadvertently obtained and appears to pertain to the commission of a crime; or
- When otherwise authorized under the ECPA.

In addition, providers of electronic communication or remote computing services are required to preserve stored communications, records, and other evidence at the request of a governmental entity, pending a court order, for up to 180 days. Governmental entities can also require providers to protect stored communications and records by making backup copies of such communications.

138. What are the protections required for transmitted communications?

To protect transmitted communications, the ECPA prohibits anyone from intentionally intercepting or attempting to intercept wire, oral, or electronic communications, or from intentionally disclosing or using or attempting to disclose or use these communications. Further, the ECPA prohibits the manufacture, distribution, possession, or advertising of any electronic, mechanical, or other device that is primarily used to intercept such communications, and imposes penalties on people who intercept or disclose communications in violation of the law. Such penalties are described in Question 139. The ECPA also prevents illegally intercepted communications from being introduced into evidence.

There are several exceptions to the rule against interception, including:

- Under certain circumstances, “in the normal course of ... employment,” an employee of a wire or electronic communication service provider can intercept communications;
- When a court order directs a provider to give assistance, or when the attorney general certifies that a court order or warrant is unnecessary;
- When the interception is not for the purpose of violating a law, and the person intercepting the communication is either one of the parties to the communication or has received permission from one of the parties to intercept the communication;
- In order for the U.S. government to conduct electronic surveillance for foreign intelligence purposes as permitted by the Foreign Intelligence Surveillance Act or other federal laws;
- When the electronic communications are readily accessible to the public, or for certain radio transmissions, such as police scanners and citizens’ band radio; and
- When the person making an oral communication has no reasonable expectation of privacy.

139. What is the penalty for violating the ECPA?

The penalties for violating the ECPA vary depending on the violation.

A person who violates Title I of the ECPA by illegally intercepting, disclosing, or using wire or electronic communications, or by making, distributing, or advertising illegal interception devices, is subject to criminal penalties, including the seizure of the equipment, a fine, and imprisonment for not more than five years. If the violation involved intercepting unencrypted communications, and was not for a tortious or illegal purpose or commercial gain, then the penalties are less severe. In addition, a person whose communications were illegally intercepted, disclosed, or intentionally used may bring a civil suit against violators. Relief includes preliminary and other equitable or declaratory relief, damages, punitive damages in appropriate cases, and attorneys’ fees and other litigation costs reasonably incurred. Damages in these suits vary based on the specific violation, but are calculated based on the actual damages sustained, or statutory damages up to US\$10,000, whichever is greater.

A person who violates Title II of the ECPA by illegally accessing stored wire or electronic communications can be fined and/or imprisoned for up to six months. If the violation is committed for commercial advantage, malicious destruction or damage, or private or commercial gain, the person can be fined and/or imprisoned for up to one year (in the case of a first offense), or fined and/or imprisoned for up to two years (in the case of any subsequent offense). In addition, parties aggrieved by access to their stored communications may bring civil suits against anyone who committed a violation “with a knowing or intentional state of mind.” Relief includes preliminary and other equitable or declaratory relief, damages, punitive damages if the violation was “willful or intentional,” and attorneys’ fees and other litigation costs reasonably incurred. Damages in these suits shall in no case be less than \$1,000 and are calculated by adding the damages suffered by the aggrieved party and the profits made by the violator.

A person who violates Title II of the ECPA by using pen registers or trap and trace devices can be fined or imprisoned for up to one year.

A good faith reliance on a warrant, court order, grand jury subpoena, or other legislative or statutory authorization may serve as a complete defense to any criminal or civil suit brought under the ECPA.

Telephone Consumer Protection Act (TCPA)

140. What is the TCPA?

The Telephone Consumer Protection Act (TCPA) has been dubbed the Do Not Call Law, because under § 227(c)(3) of the TCPA, the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) established the Do Not Call Registry, a national database of residential subscribers who object to receiving telephone solicitations.

Congress passed the TCPA in 1991 in response to concern among consumers about the growing number of unsolicited telemarketing calls they were receiving. Congress found that unrestricted telemarketing is a nuisance, can be an invasion of privacy, and creates a risk to public safety by occupying telephone lines that might be needed in an emergency. By amending the Communications Act of 1934, the TCPA employs a number of methods for reducing this nuisance, such as prohibiting businesses from using automated dialing machines to deliver unsolicited, prerecorded or artificially voiced messages (“robocalls”) to consumers; restricting advertising via fax machine; requiring the FCC to study consumer privacy and issue new rules designed to protect that privacy; and empowering the FCC to maintain a national database of consumers who object to being contacted by telemarketers (the National Do Not Call Registry).

In addition to the FCC rules adopted pursuant to the statute, the FTC has adopted the Telemarketing Sales Rules pursuant to the TCPA, including the latest amendments (which can be found at 16 CFR Part 310), which are now fully effective.

141. What are the requirements of the TCPA?

Under the TCPA and FCC rules adopted pursuant to the statute, telemarketers cannot make auto-dialed calls and calls with a prerecorded or artificial voice to emergency numbers, healthcare facilities, or to any services for which the recipient is charged (e.g., cellular phones). These calls also cannot be made to residences without prior consent. Multiple, simultaneous calls to different lines at a single multi-line business are also prohibited. In any permitted calls with a prerecorded or artificial voice, the calling entity must identify itself and give its phone number or address. Telephone lines must be released within five seconds after the recipient has hung up. Most notably, no commercial telephone solicitations can be made to residential numbers on the National Do Not Call Registry. Any telephone solicitations that are permitted under these rules, such as noncommercial calls from tax-exempt nonprofit organizations, may be made to residences only between 8:00 a.m. and 9:00 p.m. All such callers must maintain their own do-not-call lists and comply with requests by recipients not to be called again.

142. Who must comply with the TCPA?

Any person or entity making calls with an automated dialing system or an artificial or prerecorded voice must comply with the restrictions on calling emergency numbers, healthcare facilities, cell phones, and residences. Anyone making a “telephone solicitation” must comply with the rules regarding acceptable calling times, timely hang-ups, and the National Do Not Call Registry. (See Question 148 for a discussion of “Telephone Solicitation.”)

143. Who enforces the TCPA?

The TCPA provides a private right of action for the enforcement of all of its provisions. This means that any person or entity can sue in state court to enjoin another person or entity from violating the Act and to recover damages. Lawsuits to enforce the Do Not Call Registry can be brought only by a person or entity that has suffered more than one violation by the same person or entity in a 12-month period. State attorneys general may also bring enforcement suits on behalf of their constituents, except that these actions must be brought in federal court. The FCC and FTC have enforcement rights as well, and can issue warnings and impose fines for violations of the TCPA and the Telemarketing Sales Rules, but they will not recover damages for individuals.

144. What kind of damages may an individual recover from a telemarketer who violates the TCPA?

Persons who or entities that have suffered a violation of the TCPA may sue to recover either actual monetary losses or \$500, whichever is greater. If the court finds that the defendant violated the TCPA willfully or knowingly, rather than negligently or recklessly, it may increase the award by up to three times.

145. What types of defenses are available to telemarketers if they violate the TCPA?

A telemarketer does not violate the TCPA if it makes a live telephone solicitation, an autodialed call, or a call with a prerecorded or artificial voice to a recipient who gives his or her express permission to receive such a call. Live telephone solicitations, but not “robocalls,” are also permitted when made to recipients with whom the telemarketer has an established business relationship. However, even if the telemarketer has violated the rules surrounding live telephone solicitations, including the Do Not Call Registry, it can defend itself in a lawsuit by showing that it had established with due care reasonable practices and procedures designed to prevent violations of the TCPA.

146. Under the TCPA, what is the daily window of time when it is impermissible for telemarketers to place telephone calls?

Telemarketers may make telephone solicitations to residential numbers only between 8:00 a.m. and 9:00 p.m. (local time at the recipient’s location). If the number is registered on the Do Not Call Registry, no telephone solicitations may be made at any time.

147. What disclosures are required by telemarketers as part of the TCPA?

Any prerecorded or artificial message must begin by identifying the business, individual, or other entity responsible for initiating the call. During or after the message, it must state the telephone number of the responsible business, individual, or entity, and that number must be capable of receiving do-not-call requests during regular business hours.

148. Under the TCPA, what is a “telephone solicitation”?

A telephone solicitation is a telephone call that acts as an advertisement. The specific definition of “telephone solicitation” under the TCPA is “the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person ...”. Specifically excluded from this definition are messages (1) to people who have expressly consented to receive them, (2) to people with whom the caller has an established business relationship (EBR), and (3) from tax-exempt nonprofit organizations. An EBR is an existing relationship formed by voluntary two-way communication between the caller and the recipient based either on a transaction within the preceding 18 months or an inquiry or application within the preceding three months. An EBR is automatically canceled by a person’s request to be placed on a caller’s own do-not-call list.

149. What is the Do Not Call Registry?

The TCPA empowered the FCC to establish a national database of residential telephone subscribers who object to receiving telephone solicitations. Accordingly, the FCC created the Do Not Call Registry in 2003. Residential subscribers can have their home and wireless numbers added to the list at no cost by visiting www.donotcall.gov or by calling 1-888-382-1222 or 1-866-290-4326 (TTY) from the phone number they wish to register.

150. Does the TCPA pre-empt any state laws related to telemarketing?

The TCPA does not pre-empt any more restrictive state laws. However, if a state implements its own do-not-call registry, that registry must include the numbers from that state that are listed on the National Do Not Call Registry.

151. Are there any state-specific do-not-call laws?

Many states do maintain their own do-not-call registries for their residents. To find out the rules in a particular state, the FCC recommends contacting the state’s consumer protection office or public utilities commission.

152. What is the Junk Fax Protection Act of 2005?

The TCPA also places limitations on the faxing of advertisements. The Junk Fax Protection Act of 2005 (JFPA) amends and expands the rules listed in the TCPA. In particular, the JFPA codifies in the statute what had previously existed only as a regulation: the definition of an established business relationship (EBR). Before Congress enacted the JFPA, the FCC had intended to remove the EBR exception from its do-not-fax rules. The JFPA makes this exception permanent. (See Question 154 for a discussion of the EBR standards.)

153. What requirements must marketers comply with under the Junk Fax Protection Act of 2005?

Marketers cannot send unsolicited advertisements via fax unless (1) they have an EBR with the recipient, (2) they obtained the recipient's number within the context of that EBR or through a directory in which the recipient voluntarily agreed to make its number available for public distribution, and (3) the advertisement explains how the recipient can request not to receive future advertisements. This explanation must be clear and conspicuous, it must appear on the first page of the fax, and it must include telephone and fax numbers to which such a request may be sent and, if neither of these numbers is cost-free for the caller, a cost-free method such as a website or e-mail address that is available 24 hours a day. Such requests must be respected within the shortest reasonable time, but no more than 30 days.

154. What is the "Existing Business Relationship" exception under the Junk Fax Protection Act of 2005?

Marketers can send unsolicited advertisements via fax only when they (1) have an established business relationship (EBR) with the recipient, (2) get the fax number from the recipient voluntarily through the course of that business relationship or from a place where the number is published by the recipient, (3) have the required disclosures and opt-out mechanism in the fax, and (4) comply with opt-out requests. FCC regulations define an EBR for Junk Fax purposes as:

A prior or existing relationship formed by a voluntary two-way communication between a person or entity and a business or residential subscriber with or without an exchange of consideration, on the basis of an inquiry, application, purchase or transaction by the business or residential subscriber regarding products or services offered by such person or entity, which relationship has not been previously terminated by either party.



Discussion of U.S. State and Local Laws and Regulations

155. What governmental bodies have authority to enforce privacy laws and regulations?

The general trend among states is that state agencies have the authority to enforce privacy law compliance within their particular industry sector. For example, in Massachusetts, the Office of Consumer Affairs and Business Regulation promulgated a comprehensive set of regulations establishing standards for how businesses protect and store consumers' personal information. The Massachusetts Division of Banks has the power to ensure compliance with privacy laws and regulations over the banking organizations that it supervises. In Arizona, the Department of Insurance works to regulate the privacy of personal information handled by insurers. In California, the Office of Information Security and Privacy Protection is specifically designed to protect privacy rights of consumers. It is responsible for and has authority over statewide information security and privacy policies that are applicable to all state government agencies. In many states, the attorney general acts as a "catch-all" by regulating and enforcing privacy laws of other businesses that do not fall within the purview of the above governmental bodies.

156. What state laws exist related to sharing of Social Security numbers?

Many states have enacted legislative protections for Social Security numbers (SSNs). Most states, as well as the District of Columbia, currently have statutes that have some form of SSN protection. These laws vary from comprehensive to very specific statutes that protect SSNs from disclosure.

Most notably, many states have enacted laws that restrict the use and display of an individual's SSN, printing of SSNs on identification cards, and the mailing of SSNs. For example, California has a law that generally prohibits companies and persons from publicly displaying SSNs, mailing documents that display SSNs, printing SSNs on cards required to access products or services, or requiring SSNs to log on to a website. Subsequent to California's enactment of this law, several other states implemented similar laws.

Some states require that persons holding SSNs of state residents develop and maintain a privacy policy describing how SSNs are used, secured and disclosed. Connecticut, for example, requires that such a policy be publicly available; penalties for violation include fines of \$500 per violation up to a maximum of \$500,000.

157. What is California's "Shine the Light" statute?

California's "Shine the Light" statute imposes significant requirements on certain businesses that share personal information about their California customers with any other entity (whether affiliated or unaffiliated) for marketing purposes. The statute requires a business, upon the customer's request by either mail or electronic mail, to disclose

Discussion of U.S. State and Local Laws and Regulations

the types of personal information about the customer it disclosed during the prior calendar year and provide a list of names and addresses of the companies with which the personal information was shared, as well as the type of information shared with each. Categories of information include:

- Name and address
- Electronic mail address
- Age or date of birth
- Names of children
- Electronic mail or other addresses of children
- Number of children
- Age or gender of children
- Height
- Weight
- Race
- Religion
- Occupation
- Telephone number
- Education
- Political party affiliation
- Medical condition
- Drugs, therapies, or medical products or equipment used
- The kind of product the customer purchased, leased, or rented
- Real property purchased, leased, or rented
- The kind of service provided
- Social Security number
- Bank account number
- Credit card number
- Debit card number
- Bank or investment account, debit card, or credit card balance
- Payment history
- Information pertaining to the customer's creditworthiness, assets, income, or liabilities

Businesses that share information for marketing purposes must either make the disclosure on request or provide customers with a cost-free means of opting out of the sharing. Disclosures must be made within 30 days after a request, with limited exceptions. If a company does not share personal information with others (including both affiliated and unaffiliated companies), then disclosure is not required. Companies that share information for marketing purposes must also provide a disclosure of "Your Privacy Rights" or "Your California Privacy Rights" in their website privacy policy describing how customers may make requests for disclosure. They must also provide information about requesting disclosures at their places of business.

Certain limited types of sharing of information are exempted from coverage under the statute, including some types of joint marketing. Customers may bring an action for \$500 in damages for violation of the statute (up to \$3,000 for willful violations).

158. What is the Massachusetts Regulation “Standards for the Protection of Personal Information of Residents of the Commonwealth”?

The Massachusetts Regulation “Standards for the Protection of Personal Information of Residents of the Commonwealth” became effective March 1, 2010. This regulation, promulgated as part of the state security breach notification statute, requires organizations to develop, implement, maintain and monitor a comprehensive, written information security program for records containing personal information about Massachusetts residents. The regulation does not require a business presence in Massachusetts; the triggering point is the collection of personal information about a Massachusetts resident. Specifically, this regulation establishes minimum standards for the safeguarding of personal information, and applies to information contained in both paper and electronic records. Additionally, it mandates 12 specific activities that must be included in the written program. Of particular note, the regulation requires that personal information be encrypted when in transit or stored on portable devices. Oversight of vendor compliance is also required. The regulations do allow for flexibility for a business to tailor its program.

159. What is Nevada’s “Restrictions on transfer of personal information through electronic transmission”?

Nevada’s “Restrictions on transfer of personal information through electronic transmission” encryption law requires all businesses in the state to encrypt the electronic transmission of a customer’s personal information. However, facsimiles and transmissions that remain within a business are excluded from the requirement. Nevada is the first state to mandate such a specific type of security measure for customers’ personal information. Although the Nevada statute imposes strict compliance on businesses, it does not specify any penalty for noncompliance with the law.

160. What is Minnesota’s “Access Devices; Security Breach” statute? [M.S.A. § 325E.64]

The Minnesota Access Device and Security Breach law requires businesses operating within the state to enact certain minimum security measures with respect to financial data. Specifically, the law prohibits businesses from retaining credit card, debit card, or other stored-value card data for more than 48 hours after the transaction with a consumer. If a business violates that requirement and there is a subsequent security breach, the business will be liable to any financial institution that incurs costs (including fraudulent transactions) because of the breach.

161. What are some of the standards that states use to apply their privacy laws to out-of-state businesses?

It is a growing trend among states to require businesses to enact security measures in order to protect customer data. Most states, like Nevada, only require out-of-state businesses to comply with these data security laws if they are conducting business within the state.

A growing number of states are becoming stricter with regard to protection of information held by out-of-state companies. The mechanism used is to impose obligations on those holding information about state residents. Protecting state residents is within the state’s powers. As noted above, the majority of states now impose notification requirements on entities holding personal information exposed to unauthorized access or acquisition.

Similarly, many states impose requirements for the protection and security of Social Security numbers of state residents, even when companies in different states hold those numbers. Massachusetts recently enacted a personal data breach notification law and supporting regulations requiring the safeguarding of personal information stored both on paper and electronically. Any business that stores or maintains personal data about a Massachusetts resident is required to comply, regardless of whether the entity maintains a business presence within the state.

162. What are some of the current state-level trends in privacy law regulation?

A majority of states have expanded the scope of their data privacy laws to include any business that holds information about residents within the state, not just those with operations in the state. Some states, such as Alaska, Hawaii, North Carolina, Massachusetts, and Wisconsin, are also expanding regulations beyond just data held in electronic form to data in paper or any other format. States also have been enacting data security laws that contain greater specificity in terms of what security measures businesses must take. The more recent legislation in Nevada and the Massachusetts data security regulation are part of a growing trend mandating encryption of personal information.

A newly emerging trend is to include protections against medical identity theft in data security laws. In 2008, California amended the definition of “personal information” in its security breach notification statute to include medical information, diagnoses, and health insurance information related to state residents.



Intersection of U.S. Privacy Laws with Other Laws and Regulations

163. Are there any circumstances where law enforcement's interest overrides an individual's right to privacy?

Yes. Law enforcement authorities have long had the right to request financial records and other information, subject to the requirements and restrictions of the Right to Financial Privacy Act as discussed in more detail earlier in this guide. In addition, under the Bank Secrecy Act, financial institutions are required to file with the federal government reports of suspicious activity (which often contain personal information), as discussed in more detail below.

More recently, other laws have been passed that broaden the circumstances under which law enforcement may obtain sensitive information. For example, a threat to national security or suspicion of terrorist activities would allow the government to retrieve confidential information, as set forth in the USA PATRIOT Act. The Act contains certain provisions that override individuals' right to privacy, such as the National Security Letters provision, which expanded the FBI's authority to demand personal customer records from Internet service providers, financial institutions and credit companies without prior court approval.

Other such examples exist, including the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which was implemented "to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities."⁹ While there have been concerns that CALEA conflicts with Fourth Amendment rights, this Act does contain provisions enhancing privacy, including a section that raised the standard for government access to transactional data.

There has been significant debate as to whether such laws strike an appropriate balance between the legitimate needs of law enforcement and the importance of protecting individuals' rights to the privacy of their personal information. Many civil rights groups, such as the American Civil Liberties Union (ACLU), have opposed the USA PATRIOT Act because they feel that it takes advantage of individuals' civil liberties and violates their right to privacy.

164. What is the USA PATRIOT Act?

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) was passed in 2001 (following the terrorist attacks on September 11, 2001) to deter and

⁹ FCC – CALEA Information: <http://www.fcc.gov/calea/>

punish terrorist acts in the United States and around the world, enhance law enforcement investigatory tools, and provide additional requirements related to money laundering activities. Other purposes of the Act include:¹⁰

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering; and
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

165. What types of personal information may be released under the terms of the USA PATRIOT Act?

Some types of information that may be obtained by authorities under the USA PATRIOT Act include:

- Financial information (e.g., account information, transactional data, credit information, Customer Identification Program (CIP) information from banks via correspondent accounts)
- Communications information (e.g., detailed call records and voice mail records, wiretap communication information, electronic communications information)
- “Tangible items” (e.g., books, business/personal records, papers, documents, and other items in connection with a terror investigation)

166. What information triggers filing a Suspicious Activity Report?

Financial institutions are required by the U.S. Department of the Treasury to report to the Financial Crimes Enforcement Network (which is part of the Department of the Treasury) any suspicious transactions relevant to a possible violation of law or regulation. The obligation to report customer financial information on a Suspicious Activity Report is generally triggered if any of the following information is discovered:

- Any kind of insider abuse of a financial institution, involving any amount;
- Federal crimes against, or involving transactions conducted through, a financial institution that the financial institution detects and that involve at least US\$5,000 if a suspect can be identified, or at least US\$25,000 regardless of whether a suspect can be identified;
- Transactions of at least US\$5,000 that the institution knows, suspects, or has reason to suspect involve funds from illegal activities or are structured to attempt to hide those funds;
- Transactions of at least US\$5,000 that the institution knows, suspects or has reason to suspect are designed to evade any regulations promulgated under the Bank Secrecy Act; or
- Transactions of at least US\$5,000 that the institution knows, suspects, or has reason to suspect have no business or apparent lawful purpose or are not the sort in which the particular customer would normally be expected to engage and for which the institution knows of no reasonable explanation after due investigation.

“Transactions” include any deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond or other investment security, or any other payment through the financial institution.

167. What is a National Security Letter?

A National Security Letter (NSL) is a written request for information (i.e., various records and data pertaining to certain individuals) from a third party that is issued by the FBI or by other government agencies with authority to conduct national security investigations.¹¹ It requires no probable cause or judicial oversight. NSLs also contain a gag order, preventing the letter’s recipient from disclosing that the letter was ever issued to them.¹²

¹⁰ Financial Crimes Enforcement Network (FinCEN) – USA PATRIOT Act Information: http://www.fincen.gov/statutes_regs/patriot/index.html

¹¹ National Security Letters: http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm

¹² 18 U.S.C. 2709: Counterintelligence access to telephone toll and transactional records.

While considered to be a form of administrative subpoena, NSLs are ostensibly less intrusive because they are only available for authorized national security investigations (not general crime investigations) and can only be used to seek certain transactional information including:

- Financial Institution Customer Records [per the Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)];
- List of Financial Institution Identities and Consumer Identifying Information from a Credit Reporting Company [per the Fair Credit Reporting Act, 15 U.S.C. § 1681u(a) and (b)];
- Full Credit Report in an International Terrorism Case [per The Fair Credit Reporting Act, 15 U.S.C. § 1681v (via the USA PATRIOT Act of 2001)];
- Billing and Transactional Communication Service Provider Records From Telephone Companies and Internet Service Providers [per the Electronic Communications Privacy Act, 18 U.S.C. § 2709]; and,
- Financial, Consumer, and Travel Records for Certain Government Employees Who Have Access to Classified Information [per the National Security Act, 50 U.S.C. § 436].

168. Are there instances where privacy laws may negatively affect a company's efforts to comply with other mandates?

Yes. For example, financial institutions are expected to monitor their customers' transactions for evidence of potentially suspicious activity under the Bank Secrecy and USA PATRIOT Acts. In many cases, these monitoring efforts can be made more efficient and produce better results if a financial institution is able to coordinate with and obtain information from other financial institutions that have served as the counterparty for one or more of the suspect's transactions.

For example, if ABC Bank is investigating a wire transfer sent to its customer, John Smith, from his account at XYZ Bank, it would be useful for ABC to be able to obtain information from XYZ regarding whether there are any other individuals listed on the XYZ account besides Smith, the source of funds for the wire, and whether Smith has conducted similar transactions with other banks in the past. However, unless both ABC and XYZ Bank participate in and comply with the restrictions set forth in the voluntary sharing provisions of § 314b of the USA PATRIOT Act, applicable privacy regulations such as those imposed by the Gramm-Leach-Bliley Act will prohibit XYZ Bank from sharing the requested information, thereby limiting the effectiveness of ABC's investigation. In addition, privacy laws may hamper cross-border law enforcement efforts, as witnessed by the difficulties encountered by U.S. taxation authorities in pursuing investigations involving certain Swiss financial institutions.

169. Are there circumstances in which health-related information may be disclosed without the owner's permission?

In some cases, the holders of medical information may be compelled to produce such information by law. This could include, for example, a response to a subpoena. In addition, the HIPAA regulations set forth other circumstances under which health information that is otherwise protected may be shared without permission, including:¹³

- Public health authorities charged with preventing or controlling diseases, injuries, or other medical conditions, and/or with investigating a claim of child abuse.
- Persons subject to the jurisdiction of the Food and Drug Administration (FDA) for FDA-related safety assurance activities.
- Persons who may have been exposed to or are at risk of spreading a communicable disease, if the party who would share this information is authorized by law to do so.
- An employer. This is generally limited to sharing done in connection with the offering of employer-sponsored health plans and/or in connection with workplace injuries and/or surveillance of workplace safety.

Medical information contained within financial records (e.g., records of credit card transactions used to pay for medical services) is not subject to HIPAA and therefore may be shared outside of the HIPAA Privacy Rule. However, this information is typically covered under separate Gramm-Leach-Bliley Act and/or Fair and Accurate Credit Transaction Act medical information-sharing restrictions, so patients in their capacity as customers or consumers of the financial institution that maintains the record may still be able to restrict its sharing under those laws.

Likewise, medical information that is part of an educational record (e.g., a child's student vaccination history) is exempt from HIPAA.

¹³ HIPAA Privacy Rule, 45 CFR 164.512



Privacy Trends and Standards in Other Industries

170. What are some of the more significant legal risks related to privacy today?

One of the most significant legal risks is the failure to protect customer databases, which are often considered a company's most important asset. It is imperative that businesses take appropriate measures to protect against a data breach, particularly in an age of increased data sharing and electronic data formats. Businesses also should oversee the ways in which third parties are handling data, and ensure that contractual agreements are being met. Any failure by a company to keep its privacy promises to consumers poses a legal risk to the business.

Organizations also should ensure that they are abiding by all applicable data notification and collection laws and not collecting or recording information in an illegal manner. State laws vary and can create significant liability for companies when they enter a new market. Tracking privacy trends and changes in the law can help manage and mitigate legal risks that may arise.

Other legal risks include data sharing and mining, especially for marketing purposes. Businesses should ensure that their marketing departments are not using or sharing information in a way that could pose a reputational risk. Employee data can also pose a risk, especially where the information is used to discipline or terminate an employee. Companies should ensure that they utilize acceptable employee practices, maintain up-to-date handbooks, and are responsive to privacy concerns raised by employees.

Finally, companies should be sensitive to legal risks related to the improper use of information in marketing, such as in behavioral advertising or marketing by text messaging. Trends for more precisely targeted marketing can also give rise to violations of state and federal statutes prohibiting intrusion into customers' computers or Internet traffic.

171. What privacy issues surround social networking?

The rise of social networking on the Internet has led to increased risks with regard to personal data. Social networking sites include MySpace, Facebook and personal blogs, as well as applications such as instant messaging programs. Hackers often join these networks to gain access to users' personal information. Many risks posed by these sites are not new, including software attacks, phishing, disclosure of information, inaccurate information, and brand damage.

172. What are the privacy implications of cloud computing?

Cloud computing is a general concept that incorporates software-as-a-service (SaaS), Web 2.0, and other recent technology trends where the common theme is reliance on the Internet for satisfying the computing needs of the users. The service is run in a web browser on an individual's computer. The user's personal information is stored in the provider's data center. Websites such as Google, Microsoft Online, Facebook and Wesabe use cloud computing.

The concept of cloud computing is the creation of shared spaces into which people inject data. This has led to a blurring of the line between public and private spheres. Because the data is entered on a user's personal computer and uploaded to the provider's data center, it is often unclear who has access to what data. It is also difficult to track what is happening to the data. This raises questions as to whether there is a duty to investigate on the part of the outsourcer, or whether someone is responsible for cross-border issues. It is also unclear who is responsible for backing up the data and who actually owns the data.

There is also a risk of attack with cloud computing because the centralization of data creates a target for malicious users. There also might be a risk of subpoena or other government action over the information.

173. Are there any private sector initiatives to protect privacy?

Yes, there are a number of such initiatives underway or in the process of being formed. One recent example is the Information and Communications Technology (ICT) industry's Global Network Initiative (GNI), which was formed with the goal of "Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies."¹⁴

Although participation in many such initiatives is voluntary for the most part, some, such as the Payment Card Industry Data Security Standard discussed below, are much more stringent and can be functionally considered self-regulatory regimes.

174. What is the Payment Card Industry Data Security Standard (PCI DSS)?

PCI refers to the Payment Card Industry (i.e., issuers of credit, debit, prepaid, "e-purse," ATM, and point-of-sale cards), and in this context, specifically to the requirements issued by the PCI Security Standards Council (PCI SSC) to protect the security and confidentiality of credit card data. The requirements are formally called PCI Data Security Standards (PCI DSS). The PCI SSC was founded by leading credit card issuers and payment processing networks, including American Express, Discover Financial Services, JCB International, MasterCard, and Visa.

175. What types of companies are subject to PCI DSS?

Essentially, all organizations that wish to accept credit cards and other types of payment mechanisms processed by the networks named above must comply with PCI DSS. Additional requirements apply to "service providers," which, under the standards, include entities that provide credit card data storage, processing, or transmission functionality to merchants. Differing levels of requirements also apply based upon the volume of transactions conducted by a particular organization.

176. What are the consequences of not complying with PCI standards?

Fines and penalties for noncompliance with PCI DSS are established by contract with each of the individual card processing networks. In addition to fines, potential penalties can include restrictions on access to (or total exclusion from) the payment processing network(s).

177. What is NACHA?

The National Automated Clearing House Association (NACHA) – Electronic Payments Association is a not-for-profit association that oversees – and also creates, develops and enforces operating rules and business practices for – the Automated Clearing House (ACH) Network. The ACH is one of the largest electronic payment networks in the world. It processes credit transfers such as direct deposit payroll and vendor payments, and debit transfers like consumer payments on insurance premiums, mortgage loans, and other types of bills. Businesses are increasingly using ACH to collect from customers online, rather than accepting credit or debit cards.

NACHA also ensures that the ACH Network is consistent with processing payments in a secure, reliable, and efficient manner. Its other roles include:

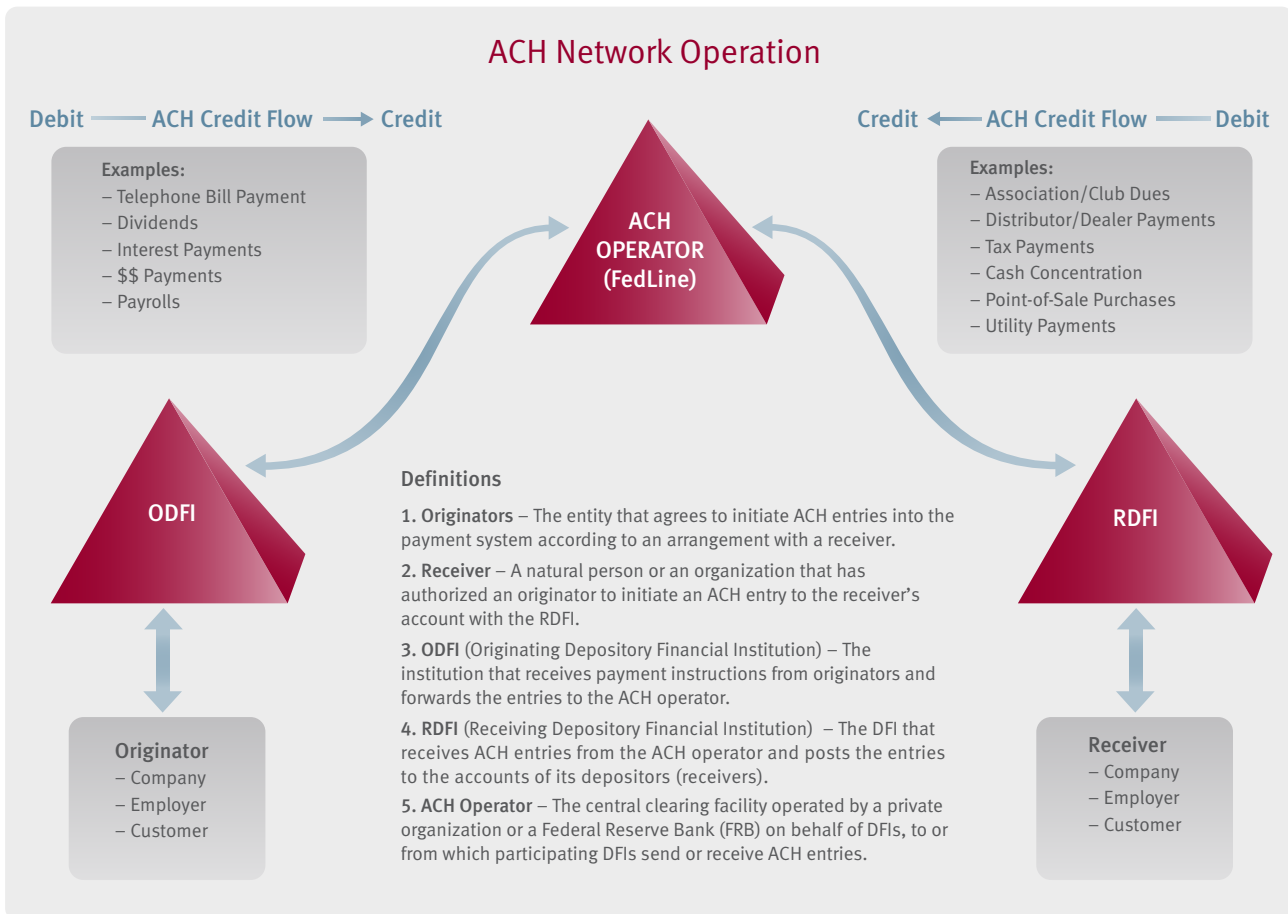
- Establishing rules and guidelines to ensure that electronic transactions are processed in a secure, reliable, and efficient manner;
- Providing education to its direct members;

¹⁴ Global Network Initiative, <http://www.globalnetworkinitiative.org/>

- Developing new payment applications;
- Implementing a risk management framework;
- Communicating best practices to financial institutions and their customers;
- Promoting the use of electronic payments through marketing efforts;
- Building relationships and responding to regulatory and government bodies and issues.

178. How does the ACH network operate?

The following illustration depicts how the ACH network operates.



179. What privacy requirements does NACHA impose?

NACHA requires its members to adhere to all applicable privacy regulations and laws. The NACHA Operating Rules also require members to use, at a minimum, a 128-bit RC4 encryption technology when banking information related to ACH is transmitted over an unsecured electronic network. NACHA does not require, but recommends, that its members utilize data security techniques in accordance with the American National Standards Institute standards.

NACHA also has an interim policy on ACH Data Breach Notification Requirements. It requires its Originating Depository Financial Institutions (ODFIs) and their originators and third parties to have proper procedures in place to prevent, detect, and investigate ACH data breach events and report such events to NACHA in a timely manner. ODFIs are also required to notify receiving institutions (RDFIs) when they experience a breach of customer-specific ACH data.

Common trends in litigation

Class Actions

- **Credit card receipts.** Following the December 2006 effective date of the amendments to the Fair Credit Reporting Act requiring truncation of credit card numbers on printed receipts, a rash of class-action lawsuits were filed claiming violation of the statute and seeking statutory damages and legal fees. These actions alleged the defendants printed more than the last five digits of the credit card or the expiration date on the credit card receipts. Damages sought varied from \$100 per transaction to \$1,000 per transaction. Class certification has been approved in several actions but denied in others on the grounds that the amount of potential damages were so disproportionate to the harm caused as to violate the due process rights of the defendants.
- **Collection of personal information in credit card transactions.** California's Song Beverly Act has seen a recent revival in class actions alleging violation of the statute. This Act prohibits any entity that accepts credit cards in full or partial payment for goods or services from either requesting or requiring that the customer provide any personal information that does not appear on the credit card in a credit card transaction. Requesting telephone numbers or e-mail addresses during the transaction has triggered class-action complaints. Recently, claims have been filed alleging that requesting ZIP codes violated the Act. Few reported decisions are available as the majority of the actions are settled.

Privacy Litigation

- **Behavioral advertising.** NebuAd Inc. and six Internet service providers were sued in the District Court for the Northern District of California for allegedly violating customers' privacy via use of deep packet inspection (DPI) technology to target advertising. The *Valentine v. NebuAd* complaint alleges that the customers were unaware their online activity was being monitored for marketing purposes. The technology allowed for identification of websites accessed, as well as information about what the customers viewed, compared and bought online, and their credit card information. Either no notice or consent was provided, or it was insufficient or misleading. The complaint also alleged that the technology intentionally negated customers' efforts to remove tracking cookies. The action alleged claims of wiretapping, forgery and browser hijacking, violating the Electronic Communications Privacy Act, 18 U.S.C. § 2510, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, California's Invasion of Privacy Act, California Penal Code § 630, California's Computer Crime Law, California Penal Code § 502, as well as aiding and abetting violations of these Acts, civil conspiracy to engage in such wrongful conduct and unjust enrichment.
- **Unsolicited text message advertising.** The District Court for the Northern District of Illinois approved a \$7 million settlement in *Weinstein v. Airit2me*. Timberland Co. allegedly contracted with Airit2me Inc. and GSI Commerce Inc. to promote a sale using conduct that involved allegedly sending tens of thousands of unsolicited text message ads to cell phones. The complaint alleged violations of the Telephone Consumer Protection Act (TCPA) that prohibits marketing calls using an autodialing system unless prior express consent is provided, and prohibits telephone solicitations to individuals on the national Do Not Call list.

Federal Trade Commission (FTC) Actions

- **Privacy policy violations.** The FTC continues to pursue complaints against entities for violating their promises in privacy policies. These include situations where promised levels of security are not provided. For example, in 2008 the FTC took action against Life is good, Inc., and Life is good Retail, alleging that the company's security claims were deceptive and violated federal law. The action was resolved by a 20-year consent decree.
- **Security breach cases.** The FTC has also taken significant actions where a security breach has exposed information in spite of promises of adequate levels of protection for that data. For example, the FTC has taken action against retailer BJ's Wholesale and processor Card Systems, alleging that the failure of both to take appropriate security measures to protect the sensitive information of millions of consumers was an unfair practice that violated federal law.
- **Violations of the Children's Online Privacy Protection Act (COPPA).** In late 2008, the FTC sued Sony BMG for improperly allowing children under the age of 13 to register on its music-based websites, saying it was in violation of COPPA. The FTC obtained a settlement, including a \$1 million fine.

180. What are the consequences of not complying with the NACHA requirements?

NACHA has established a graduated system of warning letters, and fines and other sanctions for violations of its rules, which are assessed based in part upon the severity of the violation. NACHA has also proposed to increase significantly the severity of penalties it can impose, up to and including suspending ODFI and RDFI privileges for serious violations.¹⁵ NACHA reserves the right to terminate its affiliation with any organization that violates its Code of Conduct and privacy requirements. It also reserves the right to dissociate itself from any organization that brings discredit to NACHA, or the payments profession, in general.

181. What is multifactor authentication?

Multifactor authentication is a security method where more than one form of authentication is required in order to verify a person's identity. Automatic Teller Machines (ATMs), which require both a card and a personal identification number (PIN), are one example of multifactor authentication used to ensure a higher level of security over protected information.

182. How have companies tried to educate their customers about privacy and information security?

Perhaps the most fundamental step most companies have taken is to establish their privacy policy.¹⁶ They publish this policy on their websites and frequently include it in customer mailings. To enhance their customers' ability to detect and prevent phishing, some companies have taken a number of additional actions, including providing company-specific and industrywide brochures at the time a customer relationship is established, sending periodic e-mails to warn customers of phishing attempts and other types of security risks and best practices, and even providing customers with systemic tools to detect security risks on their own (e.g., displaying a customer-selected picture or icon on secure transactional websites).

¹⁵ www.nacha.org

¹⁶ Financial institutions covered by the Gramm-Leach-Bliley Act have been required, since 2000, to adopt a privacy policy informing their customers of the institution's collection, use and disclosure of personally identifiable information. The policy must be provided at the inception of the customer relationship and annually thereafter. California law has required since 2004 that any entity that collects personally identifiable information from any California resident through a website must adopt and post a privacy policy meeting four essential benchmarks (California Business and Professions Code Sections 22575-22579).



Developing and Maintaining an Effective Privacy Program

183. What are the key elements of an effective privacy program?

While no two privacy programs are alike, common elements of all effective programs include the following:

- An accurate, well-documented, and up-to-date inventory of the organization’s actual information collection, use, storage, sharing, protection, retention, and disposal practices, as well as the laws and regulations that apply to these activities;
- Appropriate change control procedures to ensure that privacy implications are considered when new business initiatives, marketing programs, mergers and acquisitions, or other changes are contemplated;
- Clear assignment of responsibility and accountability for managing privacy-related risks;
- Appropriate involvement of and buy-in from managers of all affected departments;
- A risk-based assessment of what types of privacy policies and controls are necessary and appropriate. This risk assessment should be periodically re-performed to account for changes in a company’s business activities, as well as the emergence of new risks, new or updated laws and regulations, and other applicable external factors;
- Reducing privacy expectations and standards to clearly written policies and procedures, and making these documents available to all affected employees; and
- Performing periodic, comprehensive testing of compliance with and the effectiveness of the company’s privacy program.

184. How do you conduct a privacy risk assessment?

In general, successful privacy risk assessments utilize the following approach:

- Gather and review existing privacy policy documentation.
- Set the scope of the risk assessment, determining which subsidiaries, locations, and lines of business will be included (collectively, “the in-scope entities”), as well as what types of privacy requirements (e.g., consumer protection, employee data, and/or health insurance information) will be considered based on the requirements applicable to the company and/or its industry.
- Establish an inherent risk rating methodology, determining what factors will be considered in assessing risk and how those factors will be weighted. Some factors that might be considered in assessing risk include the volume of data collected, relative sensitivity of that data, number and complexity of the laws and regulations applicable to that data, and penalties for noncompliance.

- Prepare and/or update an inventory of the in-scope entities' information activities (note that this should potentially address information shared with company affiliates, service providers, and other third parties).
- Analyze and document the inherent risk of the information activities by entity according to the methodology defined above.
- Analyze and document the residual risk of the information activities by entity, taking into account policies, procedures, and systemic and other types of controls in place to mitigate the inherent risk identified.
- Create and execute an action plan to reduce residual risks to desired levels.
- Perform follow-up testing to ensure action plans have been timely and effectively implemented.
- Repeat the risk assessment steps described above periodically, or as significant business changes occur (e.g., mergers and acquisitions, launches of new lines of business).

185. What should privacy policy and procedures address?

Privacy policy documents should:

- Define the scope of the policy (e.g., identify to which business lines and/or employees it applies, what types of information are covered, and so on)
- Identify and describe key requirements of applicable laws and regulations, including penalties for noncompliance
- Set management's expectations for compliance, and establish enterprisewide standards, including:¹⁷
 - Information that can, must, or must not be collected
 - Restrictions on how information may be used internally
 - Restrictions on sharing information with affiliates or third parties
 - Minimum steps that must be taken to protect information, including appropriate information disposal procedures
 - How long information must be retained
 - Dispute/complaint resolution and enforcement of policy
- Assign responsibility and accountability for compliance
- Establish minimum training standards for employees subject to the policy
- Describe how, how often, and by whom compliance with the policy will be monitored
- Identify other related policies and procedures
- Establish standards for reporting to management and retaining records to demonstrate the company's compliance with privacy requirements
- Describe the process for identifying and resolving exceptions to the policy
- Establish a process to review and update the policy periodically

186. What should an effective vendor management program include?

As they relate to privacy and information security considerations, vendor management programs should:¹⁸

- Identify risks associated with vendor selection, service provision, and termination.
- Provide an outline of the process to enter into new vendor relationships, including the standards that will be used to evaluate the risks posed by a particular vendor.
- Identify the stakeholders in the vendor selection process, and identify who must approve the selection of a new, or retention of an existing, vendor relationship.

¹⁷ It may be appropriate to address certain of the elements by reference to a related policy or procedure. For example, standards for determining whether information may be shared with third parties might be addressed by reference to a separate vendor risk management policy. Retention periods might be addressed in a separate record retention policy.

¹⁸ Vendor risk management programs should also, of course, address other factors unrelated to privacy and information security, such as risks associated with the financial stability of the vendor, and the need to establish and monitor service-level standards.

- Establish the contracting process, including any baseline contractual language requirements, such as Gramm-Leach-Bliley Act (GLBA) safeguarding language for all vendors with access to nonpublic personal information (NPI), identify whether company-standard or vendor-standard templates will be used as the starting point for all contracts, address what types of modifications to standard contracts do and do not need to be presented for attorney review, and so on.
- Identify the risk-based criteria that will be used to monitor vendor and risk management controls once the relationship is underway. As a leading practice, vendors that represent higher risk from a privacy or information security perspective should be subject to ongoing monitoring for the life of the relationship, which might include some combination of (a) collecting an annual certification of the effectiveness of the vendor's privacy and information security standards, (b) asking the vendor to complete an annual survey to identify their key privacy and information security controls, (c) requiring the vendor to provide periodic independent audit or monitoring testing results related to their privacy and information security controls, and/or (d) having company personnel (or third parties engaged by the company) perform their own independent review of the security of the company's data used by the vendor.
- Establish the process for identifying, documenting, and resolving security weaknesses associated with a vendor.
- Establish procedures for contractual requirements for compliance with specific statutes and oversight of vendors providing services covered by such statutes or regulations.

187. Who in a company should “own” the privacy policy?

As with many other questions related to privacy, the “right” answer will vary significantly by company. Many larger organizations have designated a full-time chief privacy officer, who typically has a legal and/or compliance background and reports through the general counsel or chief compliance officer functions. Smaller organizations, and/or those with a lower privacy risk profile, often manage these requirements through their existing compliance and/or legal departments. Regardless of the management approach selected, however, it is critically important to ensure the involvement of appropriately senior levels of management from each of the following departments in the privacy risk management process:

- Legal
- Compliance
- Marketing and Operations
- Information Technology and/or Management Information Systems
- Facilities
- Human Resources and/or Training
- Internal Audit

To this end, implementation of an enterprisewide privacy committee comprised of representatives from the departments listed above, at a minimum, should be considered a leading practice.



Information Security

188. What is the typical relationship between a company’s privacy and information security programs?

For many organizations, the information security program (ISP) is a component of its overall privacy program, and is administered by the company’s privacy function. At a minimum, the general approach, standards, and compliance expectations set forth in the ISP should be consistent with those in the privacy program.

189. What are the elements of an effective ISP? Does it need to be a single document?

First, the ISP should be based on a comprehensive assessment of the risks posed to the company’s sensitive data, and the controls in place to mitigate those risks. Beyond that general guideline, there are a number of regulatory agency and industry standards that provide helpful guidance, or at least options to consider, with regard to the framework for and suggested components of ISPs. A few examples of these include the Federal Trade Commission’s and banking regulatory agencies’ GLBA 501b Safeguards Rules, ISO 17799, PCI, and CoBIT. In general, these standards suggest that some or all of the following elements be addressed within an effective ISP.

Common Elements of an ISP	GLBA 501b	ISO 17799	PCI	CoBIT
Management Oversight and Approval	•	•	•	•
Written Information Security Program	•	•	•	
Regular Monitoring and Testing of Systems	•	•	•	•
Training Staff to Implement the Program	•		•	•
Business Continuity Management (BCM)/ Incident Response Plan	•	•	•	
Asset Management		•		•
Access Control Measures	•	•	•	•
Physical and Environmental Control Measures	•	•	•	•

Particularly for larger, more complex organizations, it's not feasible for the written ISP to consist of a single document. Rather, the leading practice is for these organizations to implement their ISPs as a set of documents. Organizations often will create a literal or electronic binder to house these documents and demonstrate the relationship among them. These documents typically operate under a relatively brief "master ISP" that sets forth the scope of the program, defines responsibility, sets the board of directors' and management's expectations for compliance, and identifies the underlying policies and procedures that comprise the program as a whole.

A robust ISP should outline details such as how data is assessed for risk, how third parties will handle data, and how/when data storage devices such as flash drives may be used.

190. Are there any regulations that specifically require companies to implement written ISPs?

Yes. Within the United States, the FTC and banking regulatory agencies' 501b Safeguards rules have long required that written ISPs be implemented by entities subject to those rules. When the Securities and Exchange Commission's (SEC's) 501b rules were first issued, they did not contain the specific requirement that ISPs be reduced to writing; however, this requirement was added in 2004.

Additionally, as discussed in previous questions, several states (e.g., Alabama, Alaska, Georgia and North Carolina) have implemented ISP requirements for state agencies and/or other types of organizations. Beginning in 2010, Massachusetts will require any entity that holds personal information of a resident of that Commonwealth to implement a written data protection policy that includes information security.

While not specifically requiring a written ISP, a growing number of states require that any entity holding personal information about their residents adopt reasonable measures to protect that information against unauthorized access, acquisition, misuse or destruction of such information.

Further, the HIPAA Security Rule and PCI DSS,¹⁹ discussed in more detail throughout this document, also require documented information security controls.

191. If my company is not specifically required by regulation to implement a written ISP, is there any reason why we should consider implementing such a program?

There has been a strong recent trend towards the expectation that all companies that maintain sensitive information will implement adequate programs to protect this information, regardless of whether they are explicitly required to do so by law or regulation. For example, BJ's Wholesale Club, DSW, ChoicePoint, and TJ Maxx have all been charged recently with FTC security program enforcement actions due to consumer information security breaches. Most of these FTC settlements have required the affected companies to implement comprehensive information security programs and submit to biennial information security audits, at their own cost, for periods as long as 20 years.

In addition, many public security breaches have resulted in the filing of class-action lawsuits on behalf of plaintiffs who claim the company that experienced the breach had an implicit duty to protect the information with which they were entrusted, and that their failure to protect this information has resulted in harm to the plaintiffs in the form of identity theft, and the costs to review and correct their consumer report information. Certainly, being able to demonstrate that such a breach occurred in spite of a company's reasonable efforts to prevent such an action – rather than as a result of an absence of industry-standard controls – is extremely helpful in responding to such litigation.

192. What types of data should be addressed within an ISP? Do information security-related regulatory requirements apply only to consumer information, or also to information about a company's business customers and employees?

Certain laws and regulatory requirements (e.g., GLBA and HIPAA²⁰ within the United States) specifically define what type of information is subject to the requirements. Organizations subject to these requirements should, of course, ensure their ISPs effectively address risks posed to these covered data elements. However, all organizations should consider the propriety of applying the controls established in the ISP to protect other types of sensitive information, even if this information is not explicitly protected under a particular law or regulation.

¹⁹ From "Payment Card Industry (PCI) Data Security Standard, Security Audit Procedures," Version 1.1, released September 2006.

²⁰ For GLBA, see 16 CFR 313.2(n), *et seq.* For HIPAA, see 45 CFR 160.103.

193. Should the scope of an ISP be limited to electronic data?

No. Both as a matter of strict compliance and leading practice, risks to sensitive hard copy information should be considered part of a company's risk assessment process and written ISP. There have been several embarrassing security breaches caused by, for example, "dumpster diving" for printed credit reports or banking data, mailing of account statements to incorrect addresses, and other practices related to non-electronic information.

194. In some industries (notably, banking), the ISP must be approved by a company's board of directors. As a leading practice, what level of detail should be presented to the board for its review?

As ISPs have become significantly more voluminous and complex over time, many organizations have found it is unrealistic to present for board approval the entire set of documents that comprise the ISP. At a minimum, for organizations that employ the ISP binder approach described earlier, the overarching or "master ISP" document should be presented to the board for review and approval.

In addition, we have found that presenting to the board the approach followed by the organization in conducting its information security risk assessment, and the conclusions reached during the assessment, provides a valuable, straightforward means for the board to consider whether the organization is effectively managing its information security risks (which is, after all, the point of presenting the program for their review in the first place). Board members also should be presented with a summary of any security-related breaches, regulatory examination, internal audit, and/or other independent testing results, as well as the actions taken or proposed by management to mitigate the identified risks.

195. How should an information security risk assessment (ISRA) be conducted? How does the ISRA process differ from the privacy risk assessment process?

Many of the same principles discussed earlier for privacy risk assessments do apply to ISRAs as well. Perhaps the most significant difference is that ISRAs should be heavily focused not just on identifying the risks of security weaknesses, regulatory noncompliance, and so on, but also specifically on matching those risks, at a granular level, to controls in place to mitigate them. Information security-related risks also tend to evolve more rapidly (at least from an external event perspective) than privacy-related risks (which, in some cases, only change when applicable laws or regulations are revised). As a result, ISRAs should generally be re-performed more frequently than privacy risk assessments.

196. What are some of the common weaknesses and/or areas of regulatory criticism related to ISPs and/or ISRAs?

Recently, regulatory agencies have cited the following weaknesses when reviewing ISPs:

- The company's risk assessment is inadequate, and/or the results of the risk assessment process were not clearly used to shape the company's ISP
- Unclear compilation of the documents that comprise the company's ISP, and/or inconsistencies between ISP-related documents
- Failure to conduct regular, independent testing of the effectiveness of the company's ISP
- Failure to address effectively the risks posed by vendors' or other third parties' access to sensitive data in the company's risk assessment and/or ISP
- Failure to have a robust maintenance process in place for the ISP
- Lack of clear designation of ownership over the ISP

197. What types of information security requirements apply to Internet banking?

The U.S. Federal Financial Institutions Examination Council (FFIEC) issued guidance on October 12, 2005, titled “Authentication in an Internet Banking Environment.”²¹ The guidance was published for banks offering Internet-based financial services. It describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using online products and services. Regulators made clear that single-factor authentication would be considered inadequate as the sole control for high-risk transactions.

The FFIEC’s Authentication Guidance includes expectations regarding the performance of a risk assessment, account origination and customer verification, monitoring and reporting, and customer awareness. It also provides banks with a summary of common methods of authentication and verification techniques.

198. Is multifactor authentication truly required for all Internet-banking transactions?

Multifactor authentication (MFA) is a fraud deterrent designed to safeguard customer information. It requires more than one security factor to identify a customer when using an electronic banking system. There are three major types of authentication categories, including something a consumer knows (e.g., a username or PIN), something a consumer has (e.g., an ATM card or SecureID token), and something a consumer is (e.g., a fingerprint scan or other biometric device). A true multifactor authentication solution requires verification of at least one source from at least two of the three categories above.

The authentication guidance suggests that banks are expected to implement stronger authentication methods for higher-risk transactions,²² and specifically, that single-factor authentication, as the only control mechanism, is insufficient for these types of transactions. That does not mean, however, that multifactor authentication is the only alternative. Institutions may, for example, implement a layered security approach in which single-factor authentication is applied as the first stage of control, with the institution monitoring transactions and performing additional verification on large, unusual, or other higher-risk transactions, as deemed appropriate by the institution’s risk assessment.

199. Who in a company should “own” the ISP? Should the privacy and ISP owner be the same person?

Many of the same principals discussed in Question 187 (“Who in a company should ‘own’ the privacy policy?”) apply to the ISP as well. For example, the “right” answer will vary depending upon the size, risk level, and risk management structure of each organization, and regardless of the single owner designated, an effective ISP requires involvement of various management team members on a multidisciplinary basis.

That said, we offer the following points that companies may wish to consider in addressing this issue:

- There’s nothing inherently inappropriate about designating the same individual as the privacy and ISP owner, provided the individual has sufficient technical knowledge to address the ISP requirements effectively. However, as information security threats (and measures to prevent them) become more numerous, complex, and sophisticated, we expect that most larger organizations will find it difficult to identify a single individual who is and can remain sufficiently knowledgeable about both privacy requirements (i.e., those related to what types of information the company can collect, with whom it can share that information, and what types of notices it must provide) and technical information security requirements and risks.
- From a program organizational design perspective, we have found it is much more common for the privacy function to own information security than the reverse.
- For many larger organizations, a full-time chief information security officer (CISO) is the designated owner of the ISP, and reports on at least a dotted-line basis to one or more of the following people: the CIO, chief risk officer, privacy officer, and/or general counsel.

²¹ FIL-103-2005, FFIEC Guidance, Authentication in an Internet Banking Environment, October 12, 2005: www.fdic.gov/news/news/financial/2005/fil10305.html

²² “Higher-risk transactions” include those that allow access to customer-specific data, as well as those involving transfers of funds to third parties.

200. How often should a company consider reviewing and updating its ISRA and ISP?

A company should perform ongoing monitoring of the types of products and services offered and the impact of any significant changes in the company to the information security environment. As significant changes occur, the ISRA should be re-performed to focus on the unique risks. The findings of the ISRA should dictate the controls that should be implemented to mitigate these risks, and these controls should be documented within the organization's ISP.

Even if an organization does not formally evaluate every identified risk and control on an annual basis, as a leading practice, companies should at least document what steps have been taken to update their ISRAs and ISPs during the prior year, and provide a report of these activities to their senior management and board of directors. If the ISRA is not comprehensively re-performed on an annual basis, management also should have controls in place to ensure all risks are reassessed on a regular, rotational basis (e.g., all risks might be required to be assessed at least every third year, regardless of their significance).

201. What are the key risks associated with a failure to maintain an effective ISP?

The core risk of an ISP breakdown is the allowance of an information security breach, which can result in:

- The need to perform a costly process to uncover, scope, contain, and identify customers affected by the breach;
- A costly and embarrassing process to notify affected customers, potentially resulting in reputation damage and loss of business;
- Potential litigation on behalf of affected customers and/or business partners; and
- Regulatory sanctions, potentially including the assessment of multimillion-dollar fines and penalties.



Addressing Security Breaches

202. What is a security breach?

A security breach is the exposure of certain types of sensitive personal information that triggers a statutorily required notification to the individuals affected. The various states that have enacted such statutes have defined “personal information” differently, so each state’s statute must be reviewed to determine whether a “security breach” has occurred for purposes of that state’s residents.

In addition, states differ as to the extent of the exposure that triggers a “security breach,” from mere access to the data, to acquisition of the data, to risk of harm caused by the exposure. All statutes specify that the exposure must be to an “unauthorized person” in order to trigger notification. Finally, a security breach is usually defined as involving computerized or electronically stored data, but a growing number of states have expanded this to include data stored on paper, video and other media.

203. What constitutes “personal information”?

As discussed earlier in this document, “personal information” consists of an individual’s first name or first initial and last name combined with another piece of data, such as a Social Security number (SSN), driver’s license or state-issued identification number, or a financial account number (e.g., bank account, credit or debit card account number) along with any code or password required to access the account.

Most states provide that the definitions exclude information that is encrypted (either one or both of the elements); some exclude information that is redacted or otherwise made unreadable by a means other than encryption. Massachusetts has specified by regulation that 128-bit encryption is required. States permitting exclusion of redacted information have specified that SSNs be redacted to the last four numbers (Indiana, Nebraska, Ohio, Pennsylvania, Vermont, West Virginia) or redacted to five numbers (Iowa, Kansas, Oklahoma, Virginia, Wyoming); that driver’s license numbers be redacted to the last four numbers (Kansas, Nebraska, Ohio, Oklahoma, Pennsylvania, West Virginia) or to five numbers (Wyoming); and that credit cards be redacted to the last four numbers (Indiana, Iowa, Kansas, Nebraska, Ohio, Oklahoma, Pennsylvania, West Virginia) or redacted to five numbers (Wyoming).

Some states have expanded this general definition to include additional data points that, when combined with a name, may trigger a disclosure requirement. This can include medical information (California and Arkansas); employee identification number (Nevada, North Dakota); passport number (North Carolina, Oregon, Rhode Island); biometric information, such as fingerprints, iris or retina image (Iowa, Nebraska, Wisconsin); DNA profile (Wisconsin); mother’s maiden name (North Dakota); telephone number (District of Columbia, Rhode Island); electronic signature (North Dakota); or other information (North Carolina includes additional types of information if it is used to access financial resources including biometrics, passwords, mother’s maiden name; Rhode Island includes any information that identifies, relates to, describes or is capable of being associated with a particular individual including, without limitation, name, signature,

SSN, telephone number, passport number, insurance policy number, education, employment, and employment history, in addition to financial information). The District of Columbia requires notification where the data point is combined with either the name or telephone number or address of a District resident.

204. Which definition applies in my situation?

Each state's statutes apply to the data of residents of that state. As a result, the applicable law will be the law of the state of residence of the affected individual. Where the data exposure involves residents of multiple states, then the laws of each of those states must be reviewed and compliance with each must be achieved. The location of the party suffering the breach and the location of the breach incident do not affect the definitions to be used.

205. How many states have a data breach notification law? What are some of the differences among the data breach notification laws enacted by these states?

As of January 2010, 45 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws addressing exposure of personal information of residents of that state. Alabama, Kentucky, Mississippi, New Mexico and South Dakota do not currently have such laws in place.

California was the first to enact a data breach notification law; thus many of the states adopted the core of California's law. There are, however, notable differences among the states that have enacted such laws. For instance, most, if not all, of the security breach laws define "personal information" as a person's name together with an identifying data element such as a Social Security number, driver's license or identification card number, or financial account number (credit or debit card number, bank account or other financial account number). Other states have expanded "personal information" to include account passwords or access codes, digital signatures, medical/health information, biometrics, or passport or taxpayer ID numbers.

Most states' statutes address computerized or electronic information; however, the recent trend is to include information in any format. Five states (Alaska, Hawaii, Massachusetts, North Carolina, and Wisconsin) have included information in any format in their security breach statutes.

There are also several notable differences with respect to notification requirements. Many states require notification when personal information has been either accessed by or acquired by an unauthorized person. Some states only require notification of a breach if the company responsible for the data believes there is a reasonable possibility that the breach will lead to harm, injury, fraud or identity theft. Furthermore, if personal data has been compromised, all data breach notification laws require companies to notify individuals directly in writing, by telephone or, in certain cases, by e-mail. However, some states require additional notification to the attorney general or a central state office or the Credit Reporting Agencies. Most states require notification within a "reasonable" time, but others have specific timelines.

206. Is there a federal law requiring notification for security breaches?

A bill was introduced in the U.S. Senate on January 6, 2009, for a federal security breach statute, but it has not yet moved through the Congress and the potential for passage is unknown. Similar legislation had been introduced in prior Congresses without passage. There are statutes or regulations in certain sectors that require notification of security breaches. These include the recent FTC regulations regarding HIPAA information breaches and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice applicable to financial institutions covered by the Gramm-Leach-Bliley Act.

207. Is "computerized information" limited to a database in a computer or on a server containing personal information?

No. Computerized information includes any type of electronic storage that can be read using a computer. This can include information stored on files burned to CDs or DVDs, flash drives, or other portable media.

208. What is the difference between data that is “accessed” and data that is “acquired”?

Acquisition of data generally means that the data has been taken, whether this is accomplished by copying, duplicating, or downloading the data. Access to data has a broader scope and includes the potential for seeing or viewing the data by gaining access to system areas where the sensitive databases are maintained.

Forensic experts are often helpful in determining whether certain files have been accessed or whether the information contained in them has been acquired. Sometimes, this investigation can lead to information indicating that the suspicious activity was not directed at obtaining the sensitive data, but rather for some other purpose, such as to hijack a website to share pirated video or audio files, where the intrusion is harmful to the company and potentially illegal, but where notification of individuals is not triggered.

209. What about data that is “lost”?

The determination should focus on whether the data could be accessed, acquired or misused by an unauthorized person. Most statutes require a reasonable belief that the information has been accessed, acquired or misused. In the investigation, a forensic expert may be needed to assist in making this determination. When data is “lost” by an electronic process that damages or destroys the data, such as overwriting on a computer system, the data may not be accessible to an unauthorized person. However, when a computer or device is stolen, the data may also be considered “lost.” But the data on the machine or device could still be accessed, acquired or misused by an unauthorized person if the machine or device is recovered by or is in the hands of someone who can operate the device or open the stored files.

There also may be circumstances where computerized data is on devices or media that are misplaced, such as backup media that is “lost” when being transported from one place to another, or a CD containing data that is placed into a storage facility that misplaces the CD and cannot locate it when a retrieval request is made. These situations require special attention in the investigation stage to examine the level of risk that the data could be accessed or acquired by an unauthorized person. For instance, is there tracking data available that indicates whether the movement of the media can be traced, or is there any evidence of malfeasance or destruction of the media? There also may be situations where the media holding the data is physically destroyed or damaged, which may result in the data being “lost” (e.g., hard drive being crushed, a CD being broken into pieces). In such cases the potential for an unauthorized person accessing or using the data may be extremely low or impossible.

210. How do I discover a security breach?

A security breach that occurs when an electronic file is accessed can be discovered in a variety of ways. Technical alarms for unauthorized intruders are often the first line of defense, especially when the intruder enters through a web portal. An increase in website activity or a prolonged site visitor may indicate an intrusion. Theft of physical equipment or media is usually detected through physical security alarms. These protections and alarms should be part of a company’s physical security and information security plans. Some breaches are discovered when the unauthorized person who accesses the data discovers the sensitive data and reports to the company, such as when equipment is sold without stripping the data from the equipment and it is inadvertently accessed.

211. What steps should I take when I first learn that there may be an intrusion into our system or a loss of data?

No security breach incident should be “managed” by a single team member; this will avoid misinterpretation of a serious event. The security breach incident response plan should designate point people for investigation, consumer communications, regulator communications, law enforcement coordination, contract/legal/insurance review, and restoration of system integrity. The team should be pulled together immediately to respond to the incident.

Third-party subject-matter experts should be engaged early to support the incident response team. Many companies utilize outside consultants to support the team with legal, forensics and technical support.

The first steps should be to quarantine the portion of the system where the intrusion occurred and to preserve the system for forensic examination. If the intrusion was into an operating system, this may entail shutting down the system or a portion of the system for a period. If the intrusion is into a website, the site may need to be taken off-line. If the loss of data is the result of a physical intrusion into a storage area (such as where equipment is stolen or tampered with) the area should be quarantined for forensic examination.

The impulse to examine the system immediately should be tempered because an inexperienced person could overwrite the “footprints” of the intruder inadvertently, making the ultimate investigation inconclusive and the decision as to whether notice is required much more difficult. It can also hamper law enforcement’s ability to investigate and prosecute. Forensic experts can make an image of the computerized system to preserve any evidence of the intrusion. Once an image is made, the system can be placed into service again and the evidence of the intrusion will be preserved.

In addition, any and all logs, backups or other records of access to the system should be preserved so they are not overwritten, and any types of surveillance should be similarly preserved. Each system should be analyzed to determine the nature and scope of compromise. Access to the system should be restricted until it can be imaged or until the investigation is completed (if the system is not imaged). Any security gaps should be repaired and all injected malware must be located and removed.

Each step of the investigation should be documented, including the sequence of the intrusion/event and all remedial steps taken. Some states (Alaska, Florida and Iowa) require that incident documentation be retained, in some cases up to five years after the event.

Once system security and integrity are restored, the system should be tested to ensure all gaps are closed. Outside consultants can apply tests using current intruder and vulnerability management techniques.

Following the response and notification to the affected individuals, a review of the company’s policies should be conducted. If employees were involved, human resources personnel should consider providing additional training or conducting additional employee screening policies. If vendors were involved, contracts with affected and other vendors should be reviewed and any revisions or modifications initiated. In addition, insurance coverage from vendors and the adequacy of the response by the vendor should be reviewed.

The company’s response procedures and protections should also be reviewed in a “post-mortem.” This includes reviewing the company’s insurance coverage and recommending changes or additional coverage areas, reviewing responses from affected individuals to evaluate and improve communications in future events, reviewing press coverage to evaluate and improve future communications, reviewing and evaluating the overall response effort for effectiveness and to determine additional actions or policy changes that should be taken to prevent future incidents or make responses more efficient.

Finally, the company should review, evaluate and update its privacy and data protection policies, its security breach incident response plan, and accompanying basic documentation.

212. An employee accessed the database. Can that be a security breach?

A security breach involves “unauthorized” access, acquisition or misuse of personal information. Therefore, an employee who does not have authorization to access, acquire or use the data would qualify as an “unauthorized person.” Similarly, an employee who has authority for one purpose (e.g., payroll processing), but who accessed the database for a different purpose (to see where direct deposits are made) would similarly qualify as an “unauthorized person.” Most state statutes provide an exception for “good faith” situations, where an unauthorized employee mistakenly, but in good faith, accessed the data, so long as there is no further dissemination of the data.

213. Who should be involved in the investigation process?

The most efficient means of addressing a security breach is the team method. A team of employees representing five key areas and external experts in four additional areas is recommended. The names and contact information, including contact numbers outside business hours, should be included in your security breach incident response plan. Maintaining a fairly static team will help response efficiencies.

The internal team should be led by a representative of the internal legal department (or outside counsel if the company does not have an internal legal department) in order to preserve the attorney-client and work product privileges. It should include a representative from the executive team, human resources (this is key when an employee is involved), information technology/information security (to lead and direct the technical examination), risk management/compliance (to address compliance and insurance issues) and public relations (to control the message to the press). Depending on the size of the organization, one person may fill multiple functions on the team.

The external team should include outside legal counsel (with expertise in responding to security breaches and contacts in law enforcement and state agencies), forensic experts (bringing up-to-date knowledge on such incidents and providing independent reporting and, if required, testimony as well as remedial steps to enhance security), law enforcement (Secret Service or state or local law enforcement, depending on the nature of the incident) and credit card associations (which have risk management arms to follow and investigate credit card fraud).

214. When should I call law enforcement?

Law enforcement should be notified when the incident involves theft of data or other criminal acts. Some states have special task forces designated to respond to computer crimes, such as California's Computer Crimes Task Force. Some states require notification to law enforcement. Other states require that law enforcement be involved in any decision not to provide notification to individuals.

215. Who should be called?

When credit card or financial account numbers are involved, the Secret Service or local FBI office should be contacted. You will be directed to the appropriate personnel. When other data are involved, or if equipment is stolen or vandalized, local law enforcement should be contacted. Your security breach incident response plan should list the contact information for these agencies so they are at hand in the event of an incident.

216. Is there a time limit on when I have to send out the notices?

Three states, Florida, Ohio and Wisconsin, require that notification letters be sent within 45 days after discovery of the incident. Florida imposes financial penalties of up to US\$500,000 per incident for delayed notification. New Jersey regulations require that the New Jersey Division of State Police be notified within 48 hours of the discovery of a breach affecting New Jersey residents. While not statutorily required, California's Office of Privacy Protection recommends that the notice be sent within 10 business days of the discovery of the incident.

In addition, it is clear that affected individuals appreciate timely notification, based on surveys conducted of individuals who have received such letters. It is critical, however, to complete the investigation so that the notice letters are sent to the appropriate individuals and contain accurate information about the incident.

217. What if I don't have sufficient contact information to send a letter?

Each state requires that notification be given directly to the individual affected. Most states specify written notice; some specify to the last known address in the records of the company suffering the breach, and at least Maine requires that the letter be sent using first class mail. Wisconsin permits notice by any method previously used to communicate with the subject, or notice by method reasonably calculated to provide actual notice to the subject.

When there is insufficient contact information, or if the number of affected individuals exceeds a statutory threshold, "substitute notice" can be provided. In most states, "substitute notice" includes all of the following: e-mail notification (where available), posting information about the incident prominently on the company's website, and notification through "major statewide media." Notification through media outlets should be coordinated with the company's public relations specialists.

218. Can I send notice by e-mail if I have an e-mail address?

Some states permit notification by e-mail, but only if the individual has complied with the requirements of the Electronic Signatures Act (E-Sign) and agreed in advance to receive notifications by electronic means. Indiana, Virginia, and Wyoming permit e-mail notification. Alaska, the District of Columbia, Iowa and Ohio allow notification by e-mail without regard to E-Sign compliance if it is the primary means of communicating with the resident. New York permits e-mail notification if the person has consented and a log is kept.

219. Can I give notice by telephone?

Most states do not permit notification by telephone. However, 15 states do permit notification: Connecticut, Delaware, Hawaii, Idaho, Indiana (fax permitted as well), Montana, Nebraska, New Hampshire, New York (provided a log is kept), Ohio, Oklahoma, Pennsylvania, Vermont, Virginia and West Virginia. Oregon permits telephonic notice provided the affected individual is directly contacted.

220. What information needs to be included in the notice letter?

With some variance among the states, most notification letters must contain a brief description of the incident including the type of information exposed and the timing of the incident and discovery of the breach, a description of what has been done to prevent future occurrences, information regarding obtaining information from the three consumer reporting agencies, and contact information for the company that suffered the breach.

Some states specify statutorily required language regarding the availability of security freezes on consumer report accounts (e.g., Massachusetts, West Virginia); some states specify that the notice must include an admonition to review and monitor consumer report and credit information for 12 or 24 months (e.g., Hawaii, New York, North Carolina). Massachusetts prohibits disclosure of the nature of the incident to the affected individuals, but requires information regarding security freezes and obtaining a police report. It also requires that information about the incident and remedial steps be provided to the state attorney general and Office of Consumer Affairs and Business Regulation. Because of the variances between the state-mandated notice obligations, companies should carefully review the state statutes of each of the states in which affected individuals reside.

If the company is establishing a call center or specific website for further information, the contact information should be included in the notification letter. If the company is offering credit monitoring, identity theft insurance or other protections for the affected individuals, that information also should be included. It is also helpful to include a draft notification letter meeting the requirements of the states with statutory notice rules in the security breach incident response plan.

221. What is “substitute notice”?

When there is insufficient contact information, or if the number of affected individuals or the cost of providing notice exceeds a statutory threshold, “substitute notice” can be provided. (See Question 217 for more details.)

Thresholds for providing “substitute notice” will be determinative if the notifying entity has sufficient contact information to provide written notice to each individual, but wants to provide a broader type of notification instead of sending individual letters. These thresholds span a broad range from as few as 1,000 to as many as 500,000 individuals and with costs between \$5,000 and \$250,000 required before substitute notice may be given:

- \$5,000 or 1,000 individuals (New Hampshire)
- \$5,000 or 5,000 individuals (Vermont)
- \$25,000 or 50,000 residents (Idaho, Rhode Island)
- \$50,000 or 100,000 individuals (Arizona, District of Columbia, Oklahoma, Virginia)
- \$75,000 or 100,000 individuals (Delaware, Nebraska)
- \$100,000 or 5,000 individuals (Kansas)
- \$100,000 or 175,000 individuals (Pennsylvania)
- \$100,000 or 200,000 individuals (Hawaii)
- \$150,000 or 300,000 individuals (Alaska)
- \$250,000 or 250,000 residents (Colorado)
- \$250,000 or 300,000 individuals (Iowa)
- \$250,000 or 350,000 individuals (Oregon)

- \$250,000 or 500,000 individuals (Arkansas, California, Connecticut, Florida, Georgia, Illinois, Indiana (residents), Louisiana, Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Tennessee, Texas, Washington and Wyoming (or \$10,000 for Wyoming residents and 10,000 Wyoming residents))

Additionally, West Virginia permits substitute notice if the cost of providing notice exceeds \$50,000. Utah permits notification by newspaper in all cases. It also should be noted that Nebraska provides for special rules for companies with less than 10 employees. Notification through media outlets should be coordinated with the company's public relations specialists.

222. Is notice limited to cases where the information is known to have been misused?

No. In six states (Arizona, Hawaii, Kansas, North Carolina, Pennsylvania and Wyoming) the trigger for providing notice includes misuse of the information, and five states provide an exception if the incident does not create a material risk of identity theft or fraud (Massachusetts, Ohio, Virginia, West Virginia and Wisconsin), but these are in the minority. Most states require notification when there is a reasonable belief that the information has been accessed or has been acquired by an unauthorized person.

223. What protocols should be in place to make the response more efficient?

A written security breach incident response plan may be required by regulators (e.g., Massachusetts; FTC ID Theft Red Flags Rules) and will focus the response team's efforts. It should include contact information for all team members, card associations, law enforcement, regulators, forensic consultants, outside legal, call center vendors, and identity theft insurance or credit monitoring services. It also should provide an outline of the steps to be taken when an incident is discovered, including preservation of evidence of the incident, and collection of information to aid in the notification process and to identify the scope and breadth of the incident. Having prepared basic response documentation that can be tailored to address a specific incident that occurs also aids the efficiency of the response. This includes a basic notification letter (be sure to include all information required by various states, leaving only the introductory paragraph describing the incident to be inserted); basic FAQs (include resources for individuals whose credit cards, bank account information or SSNs were exposed), and a step-by-step explanation on how to place a freeze on their credit reports), and a basic press release.

In anticipation of a breach, it is good practice to test and verify the company security systems, backup/archive systems and media, and to periodically review privacy and data protection policies and promises and ensure compliance.

224. Is a call center required?

A call center may be advisable (though not "required") when a large number of individuals is affected. A number of companies provide such services with calls taken either within the United States or offshore. If a call center is to be engaged, detailed scripts including frequently asked questions and responses should be an essential part of the service.

225. Is the response different for different types of information (e.g., Social Security numbers vs. driver's license numbers)?

None of the statutes requires a different response for different types of information. However, when credit card information is exposed, the card associations and Secret Service should be contacted immediately. They may have additional information regarding the incident and bring special resources to the response effort. Because the Social Security number (SSN) is the keystone to an individual's credit, incidents involving the exposure of SSNs should be treated with sensitivity to that fact. When a significant amount of data about an individual is exposed (multiple data points or additional non-triggering data, such as date of birth or address) which increases the risk of identity theft, additional protections such as credit monitoring may be considered, though such protections are not required by statute.

When the breach has occurred and the company's privacy policy has promised a certain level of security, there is additional exposure in the form of an action for deceptive practices either under the Federal Trade Commission Act or under individual state deceptive practices statutes.

226. Which state or local agencies must receive notice?

Certain states require that particular state law enforcement or other state agencies must be notified of a security breach incident affecting that state's residents. In some cases this notification is triggered by the number of affected individuals, but not in all cases. Most of these states have special forms of notice that must be submitted and require a description of the event, the number of residents affected, and the steps taken to remedy the breach and to correct the system:

- Alaska, Connecticut, Florida, Iowa and Rhode Island (any decision *not* to notify on grounds of lack of reasonable likelihood of harm must be made after consultation with law enforcement)
- Maine (notice must also be given to the Maine Attorney General's Office)
- Maryland (notice must also be given to the Maryland Attorney General's Office)
- Massachusetts (notice must also be given to the Office of the Attorney General and Office of Consumer Affairs and Business Regulation)
- New Hampshire (notice must also be given to the New Hampshire Attorney General's Office)
- New Jersey (notice must be given to the New Jersey Division of State Police (within the Department of Law and Public Safety) for investigation and handling *before* any notice is sent to affected individuals)
- New York (notice must also be given to the New York Attorney General's Office, the New York Consumer Protection Board, *and* the New York State Office of Cyber Security and Critical Infrastructure)
- North Carolina and Hawaii (both require notice to the state consumer protection division but only if more than 1,000 persons are to be notified)
- Puerto Rico (notice must also be given to the Puerto Rico Department of Consumer Affairs)
- Virginia (notice must also be given to the Virginia Attorney General's Office)

In addition to notification of certain state agencies, 19 states require notice to be given to the three national consumer reporting agencies (Equifax, Experian and TransUnion) when a threshold number of individuals (mostly residents of the state) are notified.

Per Montana law, if a business discloses a security breach and gives a notice that suggests the individual may obtain a copy of his or her file from a consumer credit reporting agency, the business shall coordinate the notice process with the agency. Hawaii, North Carolina, Oregon, Virginia, West Virginia and the District of Columbia require notice to the consumer reporting agencies if more than 1,000 "individuals" are affected without regard to state of residence. The balance of the states focus on the number of their residents who are affected: Alaska (1,000), Colorado (1,000), Florida (1,000), Georgia (10,000), Indiana (1,000), Kansas (1,000), Minnesota (500), Nevada (1,000), New Hampshire (1,000), New Jersey (1,000), New York (5,000), Ohio (1,000), Oregon (1,000), Pennsylvania (1,000), Tennessee (1,000), Texas (10,000), Vermont (1,000) and Wisconsin (1,000).

In Massachusetts, the Director of the Office of Consumer Affairs and Business Regulation is required to give notice to the consumer reporting agencies once it receives notice from the entity suffering the breach.

227. I maintain or have licensed someone else's data. Am I required to give notice?

Entities that license or hold someone else's data are generally required to give notice of any breach in the security of their system to the owner of the data.

228. What are the penalties for not complying with the law?

In many states a violation of the law constitutes a deceptive practice or an unfair business practice. These statutes may provide for enforcement by the state's attorney general for injunctive relief or civil penalties and also may provide for a private right of action by the individual affected. Some states impose financial penalties on entities that fail to provide notice. Financial penalties will apply according to the number of residents in the affected state, so they can be cumulative. Financial penalties can range from \$100 to \$5,000 per violation (each individual) plus attorneys' fees, costs and other direct damages to state maximums ranging from \$10,000 to \$500,000. Rhode Island provides for a statutory recovery of \$500 for an affected consumer, plus attorneys' fees.



What Do You Do If You Are the Victim of Identity Theft?

229. What are the steps I should take if I am a victim of identity theft?

There are four steps consumers should take if they believe they are a victim of identity theft.²³ A consumer should keep a record of all conversations and maintain copies of all documentation resulting from following these steps:

1. *Contact a consumer reporting agency to place a fraud alert on your credit reports and review them for unusual activity.*

A fraud alert can help prevent any further accounts from being opened in the consumer's name by an identity thief. There are three consumer reporting companies who can place a fraud alert on a consumer's credit report. The consumer only needs to contact one of the three companies to place an alert; each company is required to contact the other two, which will then place the alert on any other versions of a consumer's credit report. Following is contact information for the three national consumer reporting agencies in the United States:

Equifax: 1-800-525-6285

P.O. Box 740241

Atlanta, Georgia 30374-0241

Experian: 1-800-EXPERIAN (397-3742)

P.O. Box 9532

Allen, Texas 75013

TransUnion: 1-800-680-7289, Fraud Victim Assistance Division

P.O. Box 6790

Fullerton, California 92834-6790

Once consumers place a fraud alert on their credit report, they are entitled to one free credit report from each of the above agencies. Once the credit reports are received, they should be reviewed carefully for any unexplained inquiries from companies that were not contacted by the consumer, accounts the consumer did not open, and unknown debts on the consumer's accounts. Additionally, the consumer should verify that all personal information is correct, such as address(es), Social Security number, name or initials, and employer.

2. *Close the tampered with or fraudulent accounts.*

Consumers should contact the security or fraud department of all companies and institutions affected by the identity theft and report the unexplained accounts. Additionally, identity theft victims should follow up in writing to each company by sending all letters and copies of supporting documents (including the identity theft report) by certified mail.

²³ From www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html

What Do You Do If You Are the Victim of Identity Theft?

They also should make sure to request a return receipt for documentary proof of both what and when the company received by mail.

Once a consumer has resolved any identity theft disputes with the company or institution, they should request a letter stating that the account has been closed and any fraudulent debts have been discharged.

3. *Contact the Federal Trade Commission (FTC) to file a complaint.*

There are three options by which a consumer can file a complaint with the FTC:

- **Use the online complaint form.**

The online complaint form can be found at

https://www.ftccomplaintassistant.gov/FTC_Wizard.aspx?Lang=en.

- **Call the identity theft hotline.**

1-877-ID-THEFT (438-4338)

TTY: 1-866-653-4261

- **Write the Identity Theft Clearinghouse.**

Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

4. *Contact your local police office, local FBI field office, or the U.S. Secret Service and file an identity theft report.*

The consumer should call the local police department, FBI field office, or U.S. Secret Service and tell them they would like to report an identity theft. If possible, the consumer should report the identity theft in person. If the consumer is not able to report the theft in person, he or she may be able to file a report over the Internet or telephone.

230. What is a fraud alert?

A fraud alert is a message that is placed on a consumer's credit report that alerts potential creditors to verify the consumer's identification before extending credit in their name.

There are two types of fraud alerts in which the consumer's personal circumstances will dictate which alert is appropriate. To place either of these alerts, the consumer reporting agency will require a consumer to provide the necessary documentation to prove their identity, which may include their Social Security number. The two types of fraud alerts are:

- **Initial Fraud Alert:** An initial fraud alert will remain in the consumer's file for at least 90 days. Consumers may wish to request that an initial fraud alert be placed on their credit report if they suspect their identification information has been or could be used fraudulently.
- **Extended Fraud Alert:** An extended fraud alert will remain in the consumer's file for 7 years. Consumers may wish to have an extended fraud alert placed on their credit report if they have been a victim of identity theft. The consumer reporting agency will require an identity theft report prior to placing the extended alert in the file.

231. What is a credit freeze?

A credit freeze (or "security freeze") is a restriction of access to a consumer's credit report. When a consumer places a credit freeze on his or her credit report, all third parties, such as potential credit lenders or other companies, will not be able to access the consumer's credit report without the consumer temporarily lifting the freeze. A credit freeze does not affect the consumer's credit score or ability to obtain his or her credit report; however, it may significantly delay the processing of a credit application.

Credit freeze laws and fees vary by state, and it is important to note that each reporting agency charges a separate fee to place, temporarily lift, or remove a credit freeze.

232. What is an identity theft report?

An identity theft report is a report made to a local, state, or federal law enforcement agency that provides a significant amount of information regarding the identity theft. The information provided should be sufficient to allow businesses and credit reporting agencies to verify the consumer has been a victim as well as the accounts and false information used in the theft.

What Do You Do If You Are the Victim of Identity Theft?

An identity theft report should be filed with a local, state, or federal enforcement agency. This may include the consumer's local police department, his/her state attorney general, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service.

Once an identity theft report has been filed, the consumer should send a copy of the identity theft report to any business and credit reporting companies involved via certified mail. The consumer should anticipate that the companies may request further records or details regarding the theft in order to verify the crime.

233. What do I do if the police only take reports about identity theft over the Internet or telephone?

If a consumer cannot make a report face-to-face, he or she may be able to file an automated police report over the Internet or telephone. It is likely consumer reporting agencies and information providers will require additional information and/or documentation of the identity theft, given that it is more difficult for these agencies to verify the information provided within an automated report.

In an effort to supplement an automated police report, the FTC ID Theft Complaint has a special section for reports that are not filed face-to-face. If a consumer files an automated police report they should complete the "Automated Report Information" section of the ID Theft Complaint and attach a copy of any confirmation of the automated filing received from the police.

234. What do I do if the local police won't take a report?

If the local police agency is reluctant to file an identity theft report, the consumer should insist that a report is filed. The following steps may help a consumer to obtain a report:

- **Provide an explanation of why the police report is important to both identity theft victims and businesses.** A consumer can provide the police agency with a copy of the "Law Enforcement Cover Letter" drafted by the FTC by going to its website: www.ftc.gov.
- **Use documentation to prove his or her case.** A consumer should provide as much documentation to the police as possible to substantiate the fact that identity theft has taken place as well as to emphasize the importance of filing a police report to protect a consumer's rights. Such documentation may include credit reports, debt collection letters, a copy of the consumer's printed ID Theft Complaint, and any other evidence of fraud.
- **Be persistent.** Continually emphasize that a police report is required for many creditors to resolve a dispute. Inform the authorities that consumer reporting agencies require a police report prior to blocking the fraudulent accounts and resulting bad debts from appearing on a consumer's credit report. A consumer may also wish to raise the issue to the fraud unit within the police department or elevate it to the local chief of police or the Secret Service (if the fraud occurred all over the country).

235. How do I prove that I'm an identity theft victim?

In order to prove that a consumer has been a victim of identity theft, he or she must provide documentation that substantiates his or her case. The following documents may help consumers to prove they have been a victim of identity theft:

- **Police report** – The police report is an important document for providing proof of the crime. Many creditors want a copy of the police report in order to absolve the consumer of the fraudulent debts. The consumer should send a copy of the police report to each of the three major credit bureaus.²⁴
- **Creditor documentation** – By law, companies are required to provide consumers with a copy of an application or other business transaction records relating to their identity theft if the consumer submits a written request and provides a police report. Consumers may be able to use an application for credit to show the signature on the application is not theirs.
- **ID Theft Affidavit** – The ID Theft Affidavit was developed through the efforts of credit grantors, consumer advocates, and attorneys at the FTC to help consumers close fraudulent accounts and remove debts that they did not initiate from their credit report. The ID Theft Affidavit is particularly useful in starting a dispute investigation process by the consumer

²⁴ From <http://www.talgov.com/tpd/idtheft.cfm>

What Do You Do If You Are the Victim of Identity Theft?

reporting agencies if the consumer does not have a police report or any paperwork from creditors. A consumer should send the ID Theft Affidavit to both the consumer agencies and creditors in this case. However, not all companies or businesses accept the ID Theft Affidavit. Rather, they require a consumer to use their forms instead. The consumer should check with the creditor prior to sending documentation to verify the requirements.

236. Should I apply for a new Social Security number?

The Social Security Administration may issue consumers a new Social Security number (SSN) in certain circumstances. However, applying for a new SSN should be considered carefully. In most cases, this difficult change is unnecessary and can potentially create new problems. Credit bureaus will often combine the credit records from a consumer's old SSN with those from his or her new SSN, causing potential creditors to find the consumer's identity suspicious and possibly fraudulent. Furthermore, in the case that a consumer's old credit information is not associated with his or her new SSN, the consumer may encounter difficulty obtaining credit due to the lack of a credit history under the new SSN. Finally, there is no assurance that a new SSN will not also be used by an identity thief. The risk of becoming a victim of identity theft, even with the new number, still remains.



International Laws and Regulations

International Privacy Background

237. Approximately how many countries have data privacy and protection laws?

Nations around the world have enacted varying degrees of laws designed to protect data privacy. For example, the United States and Europe currently represent opposite ends of the data privacy spectrum. The United States relies on a combination of legislation, regulation, and self-regulation, especially in discrete industry-related areas, rather than overarching governmental regulations. In contrast, the European approach, as set forth in the European Union (EU) Data Protection Directive, establishes a broad legislative baseline that applies whenever personal data is processed. In the Americas, some countries such as Canada and Argentina have followed the European approach.

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework falls between the United States and European approaches with a relatively hands-off approach that incorporates elements of the more proactive European model in a permissive set of principles.

The EU Directive restricts the transfer or transmission of data from the EU to any country whose privacy protections do not meet the Directive's "adequacy" standard. The APEC Privacy Framework does not include such a prohibition. It is important to note that the APEC Framework is still under development.

Approaches in other regions seem to vary between the U.S. and European frameworks. At this time, it is difficult to pinpoint how many countries have data privacy laws; however, most developed and developing countries offer some form of data privacy protections.

Although there are discussions among a number of the world's Data Protection Commissioners to introduce a global privacy standard (and at a 2009 summit in Madrid, a set of key standards that should be included in such a standard were agreed to), this type of standard is still a long way from being introduced.

238. Other than national laws, what other organizations have a role in international privacy law and policy?

There are a number of organizations not associated with nation-states that play an important role in international privacy law and policy. These organizations are described below.

European Union (EU) Organizations

European Union, European Data Protection Supervisor (EDPS): The responsibility of the EDPS is to make sure that all EU institutions and bodies respect the right to privacy when processing personal data. The EDPS works with the Data Protection Officers in each EU institution to ensure that the data privacy rules are correctly applied.

Council of Europe, Data Protection Commissioner: To secure every individual's right to privacy with regard to the processing of his/her personal data, regardless of nationality or residence, the Council of Europe developed the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." It is the only binding international legal instrument in this field that any country may join, including those that are not members of the Council of Europe.

European Network and Information Security Agency: The European Network and Information Security Agency (ENISA) was created and charged with creating a framework for analyzing data on EU-related security issues. ENISA was created as part of the European Commission's strategy to create a "culture of security." To accomplish this objective, the Commission's plans are to coordinate existing information security measures, foster a dialogue among public authorities on national information security policies, identify best practices for information security, and improve end users' awareness of security issues. ENISA will aid in these goals by considering the feasibility of establishing a security information-sharing and alert system.

Asia-Pacific Organizations

Asia-Pacific Economic Cooperation: The Asia-Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group (ECSG) creates legal, regulatory and policy environments in the APEC region to promote the development and use of electronic commerce. By endorsing the APEC Privacy Framework, the ECSG aims to promote a consistent approach to privacy, avoid the creation of unnecessary barriers to information flows, and prevent impediments to trade across APEC member economies. The APEC Privacy Framework provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspective. Progress on the implementation of the Framework includes application of the Information Privacy Individual Action Plans by 12 economies and the creation of a study group within the Data Privacy Sub-Group to analyze and identify best practices and promote the cross-border flow of information.

Asia-Pacific Privacy Authorities: Asia-Pacific Privacy Authorities (APPA) is the principal forum for privacy authorities in the Asia-Pacific region to form partnerships and exchange ideas about privacy regulation, new technologies, and the management of privacy inquiries and complaints.

Other Multinational Organizations

Organisation for Economic Co-operation and Development: The Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP) promotes an internationally coordinated approach to policymaking in relation to privacy and issues in order to help build trust in the global information society and facilitate electronic commerce. In this context, the WPISP brings together representatives from the 30 OECD member country governments, the private sector, and civil society to foster the emergence of solutions to build trust online. Much WPISP work focuses on raising awareness and exchanging information among all stakeholders with the objective of developing guidance as to how to ensure privacy and security online.

International Organization for Standardization: The International Organization for Standardization (ISO) is a non-governmental organization established for the purpose of developing worldwide standards, improving international communication and collaboration, and promoting the smooth and equitable growth of international trade. ISO standards are used by exporters and importers in both government and industry involved in engineering, designing, production, testing and manufacturing.

The ISO has the ability to set standards on data protection that may become law through national standards, due to its close links to national governments around the world.

239. How do the various national and regional privacy authorities differ?

European Union:

Previously, each European country had enacted its own legislation with respect to the automatic processing of personal data. However, the European Commission was concerned that diverging data protection legislation would emerge and impede the free flow of data within the European Union (EU). Thus, the European Commission adopted the EU Data Protection Directive. The Commission required all EU member states to adopt and transpose the Directive into national law by 1998. The Directive lays down a common set of rules, the goals of which are the free flow of personal data within the EU, the furthering of a unified European Market, and the protection of citizens' fundamental human right to privacy.

United States:

Although the U.S. Supreme Court interpreted the U.S. Constitution to grant a right of privacy to individuals, it is an implicit right. The Supreme Court ruled that there is a limited constitutional right of privacy based on several provisions in the Bill of Rights (the first 10 amendments in the U.S. Constitution). However, very few states' constitutions recognize an individual's right to privacy.

Although partial regulations exist in the United States, there is not a general law regulating personal data. Instead, the United States has adopted an ad hoc, sectoral approach to protecting personal data. For example, personal data held by third parties is generally not protected unless a legislature has enacted a specific law. Many such laws have been enacted by both the federal and state governments, including the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA), discussed earlier in this guide.

The United States tradition of a limited government enables the United States to regulate the public sector extensively, but generally prevents the federal government from limiting interactions between private citizens. However, 48 states have adopted a tort of privacy that recognizes a civil right of action for invasion of privacy, specifically, intrusion of solitude, public disclosure, false light and appropriation.

South America:

Habeas Data is a constitutional right found in several Latin American countries. It varies from country to country, but in general is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honor, self-determination and freedom of information of a person.

Asia:

Varying data protection models are found within the Asia-Pacific region. In Australia, cross-border transfer of personal information is regulated, although a reciprocity agreement exists between Australia and New Zealand. In New Zealand, privacy laws relate to collection, storage, use and disclosure of personal information. In Hong Kong, the use of data is restricted for any other purpose other than that for which it was collected or for a purpose directly related to such purpose. In China, there is no regime of data protection, although there are some data privacy laws directed at protecting domestic trade secrets.

240. What challenges exist for multinational corporations that collect data in these various jurisdictions?

Multinational corporations face a number of issues when collecting data in various jurisdictions. For the EU and Asia-Pacific Economic Cooperation, member countries or economies are permitted to enact varying standards because the laws establish a "floor" of privacy protection, which results in a wide range of requirements for corporations operating in both regions.

Asia-Pacific Economic Cooperation (APEC) Privacy Framework

241. What is the APEC Privacy Framework?

The Asia-Pacific Economic Cooperation (APEC) is an intergovernmental group operating on the basis of non-binding commitments. Twenty-one "Member Economies" work through APEC to enhance economic growth for the region and strengthen the Asia-Pacific community. In 2002, the APEC Privacy Sub-Group was formed to develop a privacy framework for the region.

Recognizing that there must be a balance between the free flow of information and privacy protections for personal information, the APEC Privacy Framework provides guidance to APEC economies that have not yet addressed privacy issues from a regulatory or policy standpoint. The Framework aids global organizations that collect personal data in APEC member economies to develop consistency within their organizations with regard to the use of that information. The APEC Privacy Framework balances information privacy with business needs and commercial interests, while recognizing cultural and other diversities that exist within member economies.

242. What are the nine APEC Privacy Framework principles?

- **Preventing Harm:** Privacy protections should be in place to prevent the wrongful collection and misuse of personal information. APEC also encourages member economies to develop remedies for when there are privacy infringements, which should be proportionate to the severity of harm that could occur from the misuse of personal data.
- **Notice:** Organizations within APEC member economies should provide clear information to consumers about their personal data collection practices and on how to contact the personal data controller. Individuals should also be informed that they may access and correct or delete personal information. Reasonable efforts should be made to ensure notice is provided before or at the time of the personal data collection.
- **Collection Limitation:** Personal information collected by organizations should be limited to that which is necessary to achieve the purpose of the collection.
- **Uses of Personal Information:** Personal information should only be used to fulfill the purpose of collection.
- **Choice:** Individuals should have the ability to exercise choice with regard to the collection and use of their personal data. Notice of their ability to exercise choice should be clear and accessible.
- **Integrity of Personal Information:** Personal information that is collected by organizations in APEC economies should be accurate, complete and up-to-date.
- **Security Safeguards:** Appropriate security safeguards should be in place to protect personal information against risks, such as loss, unauthorized access or misuse.
- **Access and Correction:** Individuals should have access to whether or not an organization holds information about them, and should have access to the personal information itself. Individuals should have the ability to challenge the accuracy of their personal data and be able to amend or delete the information.
- **Accountability:** When transferring personal information to another person or organization, the data controller should obtain consent or take reasonable steps to ensure that the recipient will protect the information in a manner consistent with the APEC Privacy Framework.

243. What are Cross-Border Privacy Rules (CBPRs)?

Cross-Border Privacy Rules (CBPRs) are a set of rules developed by individual organizations based upon the APEC Privacy Framework's principles. An organization applies them to its activities involving transfers of personal information across borders. This has resulted in better privacy protections for consumers and more efficient trade and investment in the Asia-Pacific region.

244. Who will enforce the APEC Privacy Framework?

While the Framework is intended to promote a consistent approach to data protection across APEC member economies, the privacy principles are aspirational rather than binding. Thus, no person or entity actively enforces the APEC Privacy Framework.

245. What challenges does APEC face in developing its Privacy Framework?

One of the goals of the APEC Privacy Framework is to provide consistency in data protection throughout the region. However, privacy is a cultural concept, so the definition of "privacy" varies by culture. For example, in many Asian languages, there is not even a word for privacy. Differing cultural attitudes toward privacy is one of the biggest challenges APEC faces.

246. What countries will be a party to APEC?

APEC consists of 21 member "economies" that each have multiple approaches to protecting consumers' personal data. The 13 economies participating in the APEC Privacy Framework include: Australia, Canada, Chile, Hong Kong, Japan, the Republic of Korea, Mexico, New Zealand, Peru, Taipei, Thailand, the United States, and Vietnam.

247. How does the APEC Framework differ from the European Union’s approach to privacy and data security?

The APEC Framework is a relatively hands-off approach that incorporates elements of the more proactive European Union (EU) model in a permissive set of principles.

But many differences exist between the two approaches. For example, the EU restricts the transfer of data from the EU to any country whose privacy protections do not meet its “adequacy” standard. The APEC Privacy Framework does not include such a prohibition.

Japan

248. What is Japan’s Personal Information Protection Act (PIPA)?

Under Japan’s Personal Information Protection Act (PIPA), public or private entities that handle personal data must provide individuals with notice concerning the way in which the information will be used, maintain the accuracy of the information, allow individuals to access and correct their information, and obtain consent before disclosing the information to third parties.

With respect to data security, entities must supervise employees and others who handle personal data, institute “necessary and proper” measures for preventing unauthorized disclosure or misuse, and ensure that third-party contractors protect data security. When there is a data breach, notice must be given to the affected individuals and to the appropriate government bodies.

Note that PIPA’s third-party disclosure and joint-use rules apply regardless of the jurisdiction in which the third party or joint user is located. Businesses are accountable for the acts of their delegates or joint users, even if they are located outside Japan.

249. Under PIPA, what is “personal information”?

“Personal information” is information that can identify a specific individual by name, birth date or other description. It also includes data that will allow easy reference to other information enabling identification of the individual.

250. Who must comply with PIPA?

PIPA applies to all personal information held in the public or private sectors and must be followed by all entities handling personal information databases for business purposes.

The following entities are exempt from PIPA compliance: state institutions, local public bodies, independent administrative agencies, local independent administrative agencies, and entities designated as having little likelihood to harm the rights and interests of individuals considering the volume of information and how it is used.

251. Who enforces PIPA?

PIPA is enforced in each industry sector by the relevant ministry office. For example, the Ministry of Internal Affairs and Communications (MIC) is responsible for privacy protection in the telecommunications and broadcasting sectors, and the Ministry of Health, Labor, and Welfare (MHLW) is responsible for protections related to employment, healthcare institutions and clinical research.

To implement PIPA’s data security provisions, the individual ministries have issued guidelines specifying various security control measures. The guidelines’ level of detail varies by ministry, as does the degree to which the included measures are mandatory or merely aspirational.

Penalties for noncompliance with PIPA include administrative warnings, fines of up to approximately US\$3,000 and imprisonment for up to six months. Affected individuals may also bring a private cause of action against companies that violate PIPA.

252. Are there other notable Japanese privacy and data security laws?

Yes, including the following:

Communications Interception Law: This law authorizes police and prosecutors to wiretap phones and monitor e-mail and faxes when investigating certain criminal cases. Police and prosecutors must notify individuals who have been monitored within 30 days after the investigation.

Internet Provider Responsibility Law of 2001: Under this law, Internet service providers (ISPs) will not be held liable when information hosted or transmitted via the Internet infringes on a third party's rights, unless the ISP has acted negligently.

Law Concerning Access to Information Held by Administrative Organs ("Freedom of Information Law"): Applicable to all information held by government entities, this law allows any individual or company to request government information in electronic or printed form.

Law Concerning the Proper Transmission of Specified Electronic Mail ("2002 Anti-Spam Law"): This law regulates the sending of commercial e-mails to Japanese residents by for-profit organizations and individuals engaged in business.

The Americas

253. What countries in South America have comprehensive privacy laws?

Brazil adopted Law No. 9.507 on November 12, 1997, implementing Habeas Data. Chile enacted Act No. 19628, titled *Law for the protection of Private Life*, in 1999. In 2000, the Argentinean Congress approved a new data protection act (Law n. 25,326) based on the European model of privacy laws that was implemented by regulations enacted in 2001 (Decree 1,558/2001). Paraguay enacted privacy legislation in late 2000 (promulgated by the president on January 16, 2001) that focuses on commercial information. Peru enacted a data protection law in July 2001, effective in August 2001 (Law No. 27.489[4]), regulating the incorporation of credit bureaus, the sources of information they can use without consent of the individual, the information that must be provided where the data has not been obtained from the data subject (similar to art. 11 of EU Directive) and establishing a set of data protection principles. In 2004, Uruguay adopted Law No. 17.838 on the protection of personal information used for commercial purposes, and the right of Habeas Data was adopted on September 28, 2004.

254. What is "Habeas Data"?

Habeas Data is a constitutional right found in several Latin American countries. It is designed to protect the privacy and freedom of information of individuals. In 1988, Brazil became the first country to implement Habeas Data, followed by Columbia, Peru, Argentina, Ecuador, Uruguay, and Mexico.

Habeas Data can be brought by any citizen against any register to find out what information is held about his or her person, regardless of whether the register is private or public. That person can request the rectification, update or even the destruction of the personal data held. The only person with standing to bring a Habeas Data complaint is the individual whose privacy is being compromised.

255. How are Brazil's privacy laws organized?

Despite the fact that the right to privacy is a constitutional right in Brazil, privacy law in that country is a mixture of laws covering different industries, interspersed with court proceedings and administrative rulings, resulting in a patchwork of privacy protection.

Consumer Protection

The 1990 Consumer Protection Law gives consumers access to their personal information stored in files and databases, as well as to the sources of the data. The law also requires that the personal data be clear and accurate, and shall not contain derogatory information that is more than five years old.

Technology

The Information Technology Law aims to create legal and technical mechanisms in order to protect the secrecy of private data. The Telecommunications Act of 1997 notes that users of telecommunications services have the right to privacy with respect to their personal information.

Financial Privacy

The Financial Institutions Secrecy Law requires financial institutions to maintain secrecy in their operations and services. Exemptions exist for information exchanged between financial institutions, information requested by the Federal Revenue and Customs Secretariat, or information needed to report illegal activity to appropriate authorities.

The Brazilian Supreme Court has declared that bank records are private and may only be used as exhibits in judicial proceedings if authorized by a judge. In 2006, however, the court ruled that when computers are legally seized, the information they contain might be used as evidence. Additionally, Brazil's Superior Court of Justice has decided that information contained in individual income tax declarations is private information protected by the Secrecy Law.

In 2004, the Rio Grande do Sul State Court of Justice determined that any breach of information regarding bank accounts is an intrusion into the right to privacy. Such a breach can only be justified by a plausible argument explaining the need for the information.

256. What are the notable privacy laws in Argentina?

The Personal Data Protection Act applies to personal data in both the public and private sectors. Data processors must observe limits on data collection, provide notice regarding the purposes for which the data will be used and, in most cases, obtain consent before collecting and handling personal data. The Act also contains a security provision instructing data handlers to take measures to guarantee the security and confidentiality of personal data to avoid misuse. Argentina's law has been deemed "adequate" under European Union (EU) standards – meaning that there can be unimpeded transfers of an EU citizen's personal data to Argentina.

Canada

257. What is PIPEDA?

The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada regulates all domestic or international transfers of data. PIPEDA requires entities to disclose the purposes for which information is collected, obtain the individual's consent to use the information, and provide individuals with rights to access and correct personal information. Entities that handle personal data must implement safeguards designed to protect against data loss, theft, or misuse. Safeguards should be "appropriate" in light of the sensitivity of the information and the amount, distribution, format and method of storage used for the information. Organizations must also ensure that personal data is protected when utilized by a third party.

258. When does PIPEDA apply?

PIPEDA applies to all private entities that collect, use, or disclose personal information in the course of commercial activities. Certain organizations may be exempt if they operate in provinces that have adopted legislation substantially similar to PIPEDA.

259. What is considered "personal information" under PIPEDA?

"Personal information" is any information about an identifiable individual, not including the business information about an employee of an organization.

260. How does Canada's definition of personal information in PIPEDA differ from the European Union's definition?

Under the European Union Data Privacy Directive, the term “personal data” means any information relating to an identified or identifiable natural person. It also includes data that will allow easy reference to other information enabling identification of the individual. In contrast, Canada's PIPEDA uses the term “personal information” to mean information about an identifiable individual, but does not include business information about employees of an organization.

261. What remedies are available as a result of a breach of PIPEDA?

Canada's Privacy Commissioner is responsible for investigating complaints under PIPEDA. Disputes that remain unresolved after the Commissioner's investigation may be brought before a federal court, which may award damages to the affected individual. There is currently no mandatory federal data breach notification law in Canada, although many companies voluntarily provide notification of data breaches.

262. Are there any provincial privacy laws in Canada that impose more stringent privacy standards than PIPEDA?

Yes. In Canada, every province and territory has legislation governing the collection, use and disclosure of personal information held by government departments and agencies. An independent commissioner or ombudsman oversees such legislation by receiving and investigating complaints. Most provinces also place restrictions on credit reporting agencies concerning information disclosure, and give consumers the right to access and challenge the information's accuracy. Numerous provincial laws regulate credit unions by ensuring the confidentiality of information regarding members' transactions. Finally, many provinces have enacted laws designed to protect the confidentiality of personal information collected by healthcare and other professionals.

In response to public concerns regarding the USA PATRIOT Act, a number of Canadian provinces have amended their privacy legislation to address cross-border data flows with the United States. Specifically, Alberta, British Columbia, Nova Scotia and Québec prohibit public bodies from allowing service providers to access or store personal information transferred to them in the course of providing services from a location outside Canada without the individual's consent.



European Union Privacy and Information Security Laws and Regulations – A Closer Look

The European Union (EU) Data Protection Directives

263. What are the European Union (EU) Data Protection Directives?

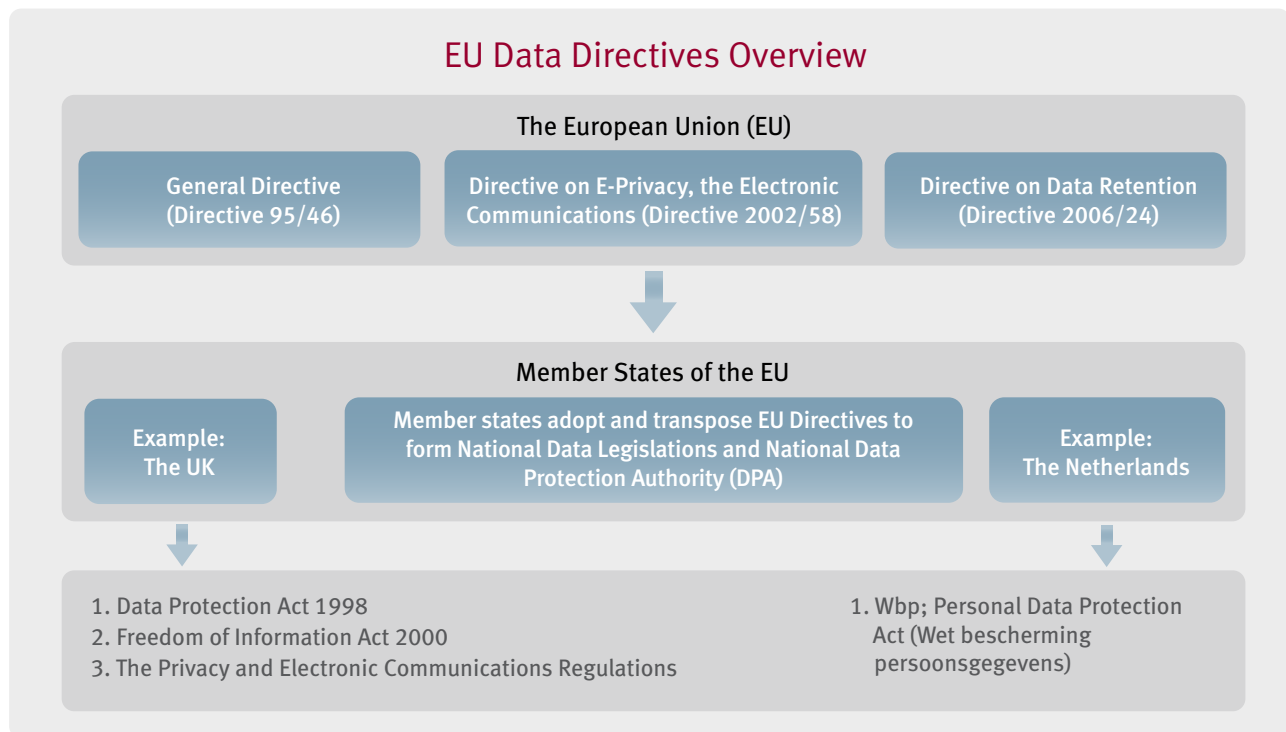
The EU is a supranational and intergovernmental union of 27 “member states” (countries) and a political body. The three primary pieces of EU privacy legislation are:

- The General DP Directive (Directive 95/46), which provides a framework for data protection (the “General DP Directive”);
- The Directive on E-Privacy Electronic Communications (Directive 2002/58) (the “E-Privacy Directive”); and
- The Directive on Data Retention (Directive 2006/24), which provides guidelines on generated or processed data retention (the “Data Retention Directive”).

Directive 95/46 was established to provide a harmonized regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries.

Directive 2002/58 complements the General DP Directive and applies to matters not specifically covered by that Directive. It deals with the regulation of a number of important issues such as electronic communications (e.g., e-mail, text message, fax, and voice mail), spam marketing and the use of cookies to collect data.

Directive 2006/24, in summary, creates an obligation for communications and Internet service providers to retain traffic and location data for the purpose of the investigation, detection and prosecution of serious crime.



264. What is the purpose of the EU General DP Directive?

The purpose of the EU General DP Directive is to “allow for the free flow of data within Europe” and to “achieve a harmonised minimum level of data protection throughout Europe.” The principles spelled out in the General DP Directive reflect these two purposes. In order for a business or organization to be able to collect personal information lawfully, a number of principles must be abided by. These principles are:

- **Fairness:** Personal data must be processed fairly and lawfully.
- **Legitimacy:** Personal data may only be processed for limited and defined purposes.
- **Finality:** Personal data may only be collected for specified, explicit, and legitimate purposes and may not be further processed in a way incompatible with those purposes or for longer than is necessary.
- **Transparency:** The data subject must be given information regarding data processing relating to him or her, and it must be processed in accordance with his or her rights.
- **Proportionality:** Personal data must be accurate, adequate, relevant, and not excessive in relation to the purposes for which it is collected and further processed.
- **Confidentiality:** Technical and organizational measures to ensure confidentiality and security must be taken with regard to the processing of personal data.
- **Security:** Personal data shall not be transferred outside the European Economic Area unless that country has an adequate level of protection in place.

265. What role do the EU member states play?

Member states are responsible for developing national legislation and creating a national Data Protection Authority (DPA) as part of their national legislation. The legislation enacted by the individual member states does not have to be completely uniform, but it does have to follow standards. The laws have to meet the minimum standards of the Directives. Ultimately, the final word in enforcement lies with the member states.

Details about the National Data Protection Commissioners can be found at the following website:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm.

266. What are a DPA's obligations?

Just as the national privacy legislation of the EU member states can differ from each other, so too can the setup of each state's DPA. The DPAs act in an advisory, investigatory and enforcement role. They give advice to individuals, organizations, firms and companies engaged in the processing and control of personal data in their countries. However, such individuals, organizations, firms and companies are not obligated to consult with their national DPA.

The DPAs are responsible for regularly drawing up a report on their activities, which is made public. The DPAs must hear claims lodged by any person, or an association representing that person, concerning the protection of his/her rights and freedoms.

267. What powers do the DPAs have?

The DPAs are endowed with the following powers:

- Investigative Powers:
 - The ability to collect all the information necessary for the performance of its supervisory duties
 - Powers of access to data forming the subject matter of processing operations
- Intervention Powers:
 - The ability to deliver opinions before processing operations are carried out
 - Ensuring appropriate publication of such opinions
 - Ordering the blocking of data
 - Erasing or destroying data
 - Imposing a temporary or definitive ban on processing
 - Warning the controller
 - Referring the matter to other regulatory bodies or the court
- Legal Powers:
 - The power to engage in legal proceedings where the national provisions adopted for the DP Directive have been violated
 - To issue fines (the levels of which are set, where appropriate, by national law in an EU member state)

268. What is the “Working Party”?

Under Article 29 of the EU Directive, a Working Party is established. It is made up of the Data Protection Commissioners from the European member states, together with a representative of the EU Commission. The Working Party is independent and acts in an advisory capacity. The Working Party wants to have consistent application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics. It also advises the EU Commission on the adequacy of data protection standards in non-EU countries.

The Working Party's full name is “Working Party on the Protection of Individuals with regard to the Processing of Personal Data.”

269. What does the General DP Directive mean to companies/organizations?

The General DP Directive places some very specific information-handling requirements on personal data any organization wants or needs to process in one of the EU countries. Organizations based within the EU must meet the requirements of the General DP Directive implemented by their respective country's data protection laws to continue doing business if it involves sharing and/or processing data with these countries. Organizations will need to:

- Understand the General DP Directive;
- Understand individual member states' data protection legislation according to the territories in which the organization operates;
- Determine what they must do to meet the requirements; and
- Implement the requirements.

270. What is considered personal data under the General DP Directive?

The General DP Directive covers information relating to “an identifiable person.” This includes information by which an individual can be directly identified. Examples include or may include: name, address, identity number and physical attributes.

The General DP Directive also recognizes that “sensitive” information may have to be processed under certain conditions (e.g. details of race, religion or sexual orientation). As this data could expose the data subject to discrimination, extra safeguards are in place to protect the processing of sensitive data.

The Directive does not apply to the processing of personal data in the course of an activity that falls outside the scope of community law or to processing operations concerning public security, defense, state security and the activities of the state in areas of criminal law, and by a natural person in the course of a purely personal or household activity.

271. What is a data controller?

A data controller is a natural or legal person, public authority, organization or any other body that alone or jointly with others has full authority to decide how and why personal data is to be “processed” (this includes using, storing and deleting the data). The controller may be a natural person appointed to a position of “controller” within a company or it may be the legal entity itself. Data controllers must implement measures appropriate to protect personal data from accidental or unlawful destruction or loss, alteration or unlawful disclosure or access.

For example, an employer is a data controller (and may be a processor) for employee data, while a retailer is a data controller (and may be a processor) for customer data. When Organization A decides that it wishes to pass the personal data it holds to another organization, Organization B, then Organization A is acting as a data controller.

Whether the receiving organization (Organization B) is also considered a data controller will depend on whether it will have the authority to decide how and why the data will be stored, used and deleted. If the receiving organization has discretion in this area, it is probably a data controller as well.

272. What is a data processor?

A data processor is a natural or legal person, public authority or organization that “processes” personal data, which may be on behalf of a data controller. Processing includes reading, amending, storing, deleting and otherwise “using” data.

For example, if Organization A (a data controller) passes personal data to Organization B, but retains the right to specify what should be done with that data, then generally speaking, the receiving organization is a data processor. Organization A is legally responsible for any breaches of the General DP Directive committed by any data processor acting on its behalf.

If information held in a company’s human resources database is passed to a payroll company to carry out payroll processing, this is done as a data controller to data processor transfer. This is because the company will retain control over the data and the purposes for which it is processed.

273. What is the difference between a controller and processor of data?

The scope of the application of local data protection law will vary depending upon whether the entity is a controller or a processor. A processor’s responsibility under local law usually is limited to following the instructions of the controller and ensuring the confidentiality and security of the data. Likely examples of processors include providers of caching services and websites hosting third-party data. In contrast, the controller usually remains accountable for the data it processes. Furthermore, the controller must register its processing activities with the data protection authorities and ensure that the data is processed in compliance with data protection laws.

274. What is a data subject?

A data subject is an individual who is the subject of personal data. For example, personal data that a company holds about customers makes each customer a data subject.

275. What is an “establishment” under the Directive?

An “establishment” under the EU’s General GP Directive is the institution, organization, firm, company, business, enterprise or other body through which the controller conducts the processing of personal data. The activities of an establishment must conform to the national laws of each EU member state, or if the establishment is in the territory of several member states, it must comply with obligations laid down by the applicable national law.

276. What constitutes “use of equipment” under the Directive?

Equipment used solely for conveying personal data through a member state is not sufficient to constitute “use of equipment” under the General GP Directive. However, use of caching servers located in a member state may trigger the data protection law depending on factors such as the member state, the data stored in the caching servers, and the interaction between the local entity and the data stored in the caching servers. Placing cookies on a user’s computer, as well as targeting websites at local users within a member state, may also be sufficient to constitute “use of equipment” and employ the local data protection law.

277. When and where are data protection rules applicable?

The EU’s data protection rules are generally applicable in the following situations:

- When the controller is established within the EU;
- When the controller is outside the EU, but uses equipment situated within the EU in order to process data; or
- When the controller is outside the EU, but processes data in the EU.

Where the controller is established in several member states, it must ensure that each of its establishments complies with the obligations laid down by the individual member state.

278. What are the rules on the processing of personal data?

The General DP Directive sets out the basic guidelines for processing personal data. However, it stipulates that, “Member States shall determine more precisely the conditions under which the processing of personal data is lawful.” Each member country has its own legislation covering the processing of personal data. Therefore, the rules for processing personal data vary from country to country. (In this FAQ guide, the processing rules for Italy, the Netherlands and the United Kingdom are examined.)

279. What are the rules on the collection of data?

The General DP Directive stipulates that in cases where data is collected directly from the data subject, the data controller must provide the following information to the data subject:

- The identity of the controller and of his or her representative, if any;
- The purpose of the processing for which the data is intended; and
- Any further information, such as:
 - The recipients or categories of recipients of the data,
 - Whether replies to the question are obligatory or voluntary, as well as the possible consequences of failure to reply,
 - The existence of the right of access to and the right to rectify the data concerning him/her.

280. What are the principles relating to data quality?

It is the responsibility of member states to ensure that the controller complies with the following data protection principles:

- Personal data must be “processed fairly and lawfully”;
- Data must be collected for “specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”;
- Collected data must be “adequate, relevant and not excessive”;

- Data must be “accurate and kept up-to-date”; and
- Data is kept in a form that “permits identification of data subjects for no longer than is necessary for the purposes for which they were collected.”

281. What are the criteria for making data processing legitimate?

Personal data may be processed only if:

- Consent has been unambiguously given by the data subject;
- Processing is required for performance of a contract that the data subject is part of;
- Steps need to be taken at the data subject’s request prior to entering into a contract;
- Compliance with a legal obligation is required;
- It is necessary to protect the vital interests of the data subject;
- It is in the public’s interest; or
- It is “in the exercise of official authority vested in the controller.”

282. What are the rules on unsolicited communications and electronic direct marketing?

The various EU Directives, primarily the E-Privacy Directive, aim to ensure that the data controller takes responsibility for data it holds on data subjects, specifically around unsolicited communications and direct marketing. These rules include the following:

- Generally speaking, only if subscribers have given their prior consent can electronic communications such as automatic calling machines, fax machines or e-mails be used for direct marketing.
- Where an e-mail address from a customer is obtained, in the context of the sale of a product or a service, the electronic contact details may be used for direct marketing of similar products or services.
- Customers must be given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.
- Unsolicited electronic communications are not allowed without the consent of the subscribers concerned.
- Companies are prohibited from sending electronic communication that disguises or conceals the identity of the sender on whose behalf the communication is made, or that does not include a valid address to which the recipient may send a request that such communications cease.

283. What are the businesses’ obligations to retain data?

Certain businesses and organizations are responsible for ensuring that certain personal data is retained for the purposes of the investigation, detection and prosecution of serious crime.

Providers of publicly available electronic communications services or of a public communications network must retain certain types of personal data including:

- Data necessary to trace and identify the source of a communication (e.g., telephone number, name)
- Data necessary to identify the recipient of a communication (e.g., phone number dialed)
- Data necessary to identify the date, time and duration of a communication
- Data necessary to identify the type of communication as well as a user’s communications equipment

284. Who should have access to retained data?

It is the responsibility of EU member states to adopt measures to ensure that data is retained in accordance with Directive 2006/24, and is provided only to the competent national authorities in specific cases and in accordance with national law.

Each member state, in its national law, defines the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements.

285. What are the retention periods?

EU member states are responsible for ensuring that the categories of specified personal data are retained for periods of not less than six months and not more than two years from the date the data was collected.

286. Are there any guidelines on data protection and data security in relation to retention?

It is up to EU member states to ensure that providers of publicly available electronic communications services or of a public communications network respect, at a minimum, the following data security principles:

- The retained data shall be of the same quality and subject to the same security and protection as data on the network;
- The data shall be subject to appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;
- The data shall be subject to appropriate technical and organizational measures to ensure that it can be accessed only by specially authorized personnel; and
- The data (except for data that has been accessed and preserved) shall be destroyed at the end of the period of retention.

Data Protection Authorities (DPAs) in each EU member state typically issue guidance or laws so these principles are achieved.

287. Should businesses ensure confidentiality of processing?

Any person who has access to personal data and is acting under the authority of the controller or the processor, including the processors themselves, must not process the data except on instructions from the controller unless they are required to do so by law.

288. How should businesses ensure security of processing?

The General DP Directive states that the controller must implement appropriate technical and organizational measures to protect personal data against the following:

- Accidental destruction
- Unlawful destruction
- Accidental loss
- Unauthorized alteration
- Unauthorized disclosure
- Unauthorized access
- All other forms of unlawful processing

Businesses must ensure a level of security appropriate to address the risks represented by the processing and the nature of the data to be protected.

289. What if data processing is carried out by a third party?

When processing is carried out on behalf of a business or organization, the controller must choose a processor, providing sufficient guarantees with respect to the technical security measures and organizational measures governing the processing to be carried out. The third party must ensure compliance with those measures.

Further, there must be a legal contract binding the processor (third party) to the controller (business or organization). The contract must stipulate that:

- The processor must act only on instructions from the controller.
- The law of the member state in which the processor is established also will be incumbent on the processor.

290. What is notification?

Notification is when controllers or their representatives alert their respective member state's supervisory data protection authority that they will be carrying out any such operation. Data controllers have an obligation to notify their relevant supervisory authority.

291. What are the contents of notification?

Member states specify the contents of notification, but they shall include at least the following under European law:

- The name and address of the controller and its representative (if any)
- The purpose or purposes of the processing
- A description of the categories of the data and data subject, or categories of data relating to them
- The recipients or categories of recipients to whom the data might be disclosed
- Proposed transfers of data to third countries
- A general description of the information, sufficient to make a preliminary assessment of the appropriateness of the measures taken to ensure security of processing

292. What are the consequences of not complying with the Directives?

Any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered. However, controllers may be exempt from this liability if they can prove they were not responsible for an event that led to the damage.

Individual member states are responsible for laying down sanctions (and the level of fines) to be imposed in cases of infringement of the provisions of the Directives. In the United Kingdom, for example, following a recent change in legislation, the level of fine that can be imposed is potentially unlimited.

293. What typical privacy policies should a business implement to maintain data privacy regulations?

Typical privacy policies that businesses and organizations should implement are:

- Acceptable use policies
- Client confidentiality policies
- Policies within third-party contracts
- Internet website policies (e.g., policy regarding use of cookies)

Additionally, procedures should be established for maintaining the privacy policy, including the following:

- Define the scope of the policy (i.e., identify to which business lines and/or employees the policy applies, what types of information are covered, and so on)
- Identify and describe key requirements of applicable laws and regulations, including penalties for noncompliance
- Set management expectations for compliance, and establish enterprisewide standards
- Assign responsibility and accountability for compliance
- Establish minimum training standards for employees subject to the policy
- Describe how, how often, and by whom compliance with the policy will be monitored
- Identify other related policies and procedures
- Establish standards for reporting to management and retaining records to demonstrate the company's/organization's compliance with privacy requirements
- Describe the process for identifying and resolving exceptions to the policy
- Establish a process to review and update the policy periodically

294. What is cloud computing and what data privacy issues are related to it?

In general terms, “cloud computing” means that a computer’s applications run somewhere in the “cloud” (i.e., on someone else’s server accessed via the Internet). Instead of running program applications or storing data on your own computer, these functions are performed at remote servers connected to your computer through the Internet.

Further, the term “cloud computing” refers to any computer network or system through which personal information is transmitted, processed and stored; typically, individuals have little direct knowledge, involvement or control over cloud computing networks or systems.

Internet search company Google Inc., for example, operates several well-known cloud computing services. It offers its users applications such as e-mail, word processing, spreadsheets and storage and hosts them in “the cloud” – in other words, on its own servers. Therefore, it is possible for users to create documents without maintaining any word processing software on their computers.

However, when users choose to store their personal data with programs hosted on another entity’s hardware, they lose a degree of control over that data. Although, generally speaking, the responsibility for protecting information from hackers and internal data breaches belongs to the hosting company (as the data controller), users should be aware of the potential risks. They should read the hosting company’s privacy policy to become fully aware of their rights.

The General DP Directive and Transfer of Personal Data to Third Countries

295. What does the General DP Directive mean to companies outside Europe?

The General DP Directive places some very specific information-handling requirements on the data any organization wants or needs to process in any country outside the European Economic Area (EEA). The transfer to a country outside the EEA of personal data may take place only if the third country in question ensures an adequate level of protection.

The Directive does not specifically define what constitutes an adequate level of protection, but it indicates that all circumstances surrounding the transfer, including the laws in force in the third country, must be considered by the supervising authority in making a determination about adequacy. (The EU Commission engages in dialogue with non-EU countries to ensure a high level of protection when exporting personal data to those countries.)

The General DP Directive also allows the European Commission to issue standard contractual clauses that those transferring data to non-EU countries can use to fulfill the requirements set down by the General DP Directive so long as the transferor and transferee have agreed to these clauses. The clauses contain obligations that each party agrees to adhere to in order to maintain the security of personal data.

Two sets of standard contractual clauses were introduced: Set I, adopted by the Commission in 2001, and Set II, which the Commission adopted at the end of December 2004. These clauses include the purpose for collecting the data, the quality and proportionality of the data that must be maintained, the transparency and security of the procedure, the rights of access to the data, and the restrictions on transferring the data to any third parties.

Currently, the only states that have been approved by the European Commission as “adequate” to transfer data freely to/from EU member states are Guernsey, Jersey, the Isle of Man, Switzerland, the United States (for corporations that have signed up and agreed to abide by the procedures/requirements of the Safe Harbor provisions), Canada and Argentina.²⁵ Once a state’s data protection legislation has been deemed adequate by the European Commission, no member state can deny the transfer of personal information to that state. Moreover, if a violation of the data protection legislation occurs, it is the responsibility of the member state, and not the European Commission, to prosecute or rectify the situation.²⁶

²⁵ Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries.

²⁶ *Negotiating Privacy: The European Union, The United States and Personal Data Protection*, p. 27-28, Heisenberg, Dorothee, Lynne Rienner Publishers, Inc., Boulder, Colo., 2005.

Case Study: A large multinational company sending French employee data to the United States

- The enforcement action against the company was related to a global human resources database.
- When the company initially registered the database as required by French law, the company stated broadly, but somewhat vaguely, that it was engaging in “data collection and processing for the purpose of ‘managing the careers of the company’s international employees.’”
- Finding this description insufficiently detailed, the French Data Protection Authority (CNIL) asked the company to provide “a description of the exact purposes for which the information was sought, the precise cases in which personal data is sent to Great Britain and the United States, exact places of installation of servers and systems, precise purpose of the data storage, exact recipients of the data, safety measures ensuring the data’s confidentiality, and the shelf life of the data.”
- The company failed to provide the requested information, forcing CNIL to exercise its authority to conduct an on-site investigation at the company’s French headquarters.
- CNIL’s investigation uncovered that contrary to the description in the company’s initial registration, the employee database was “an essential management tool, at the world level.”
- CNIL confirmed that the company was using the database to transfer human resources data to the United States, although the company had never received CNIL’s approval for the cross-border transfer of this information. In addition, the company did not explain the purposes of these transfers to CNIL.
- CNIL issued a €30,000 fine for, among other things, improperly transferring employee information to the company’s U.S. headquarters.

296. What is an “adequate level of protection”?

An adequate level of protection, while not specifically defined by the General DP Directive, is assessed in light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, including:

- The nature of the data
- The purpose and duration of the proposed processing operation(s)
- The country of origin
- The country of final destination
- The rules of law in force in the third country
- The professional rules and security measures compiled within that country

The member states and the European Commission inform each other of cases where they consider that a third country does not ensure an adequate level of protection.

297. What happens if an adequate level of protection is not in place in the third country?

Data transfer from the member state to the third country will be prohibited if the European Commission finds that the third country does not ensure an adequate level of protection. It is the individual member state’s responsibility to take the enforcement measures necessary to seek to prevent any transfer of data to the “inadequate” third country.

298. What if there is conflicting opinion between the European Commission and the member state with regard to the adequate level of protection?

The decision by the European Commission is final and member states shall take the measures necessary to comply with decisions.

299. Are there any exceptions that allow the transfer of data to a third country that does not ensure an adequate level of protection?

Transfer of personal data to a third country that does not ensure an adequate level of protection can take place if one of the following applies:

- The data subject has given consent unambiguously to the proposed transfer;
- The transfer is necessary for the performance of a contract between the data subject and the controller;
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- The transfer is necessary in order to protect the vital interests of the data subject;
- The transfer is made from a register that is intended to provide information to the general public;
- Where the contractual clauses offer significant safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals; or
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims.

Detailed information on the adequacy of the protection of personal data in third countries can be found on the official European Commission website: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

300. What options are available to organizations when transferring personal data out of EU countries?

Third-country transfers: No data may be sent from Europe unless the destination is a “third country” that “ensures an adequate level of data protection.” Only a handful of countries have received an adequacy determination from the EU.

Certifying to the Safe Harbor Accord (only for U.S.-based organizations): This is a voluntary self-certification system for transmitting data from the EU to the United States that allows U.S. data processors to receive personal data from Europe, so long as they agree to treat the data as if it is still in Europe and subject to the General DP Directive. The Safe Harbor Accord consists of seven data protection principles that the European Commission has determined provide an “adequate level of protection” for personal data. By certifying adherence to the principles outlined in the Safe Harbor Accord, a U.S. business can meet the Directive’s “adequacy” requirement, even though the United States, on a national level, does not.

Once a U.S. organization certifies it is in compliance with the principles, the data protection authority of each EU member state must automatically approve transfers of personal data to that organization. It is important to note that certification to the Safe Harbor Accord constitutes an actionable, public representation to the U.S. government that the organization will adhere to the promised privacy protections and, therefore, is subject to administrative enforcement by the U.S. Federal Trade Commission. The organization also must agree to cooperate with EU member states’ data protection authorities and abide by their enforcement orders.

Binding Corporate Rules (“Code of Conduct”): Binding Corporate Rules (BCRs) are corporate codes of conduct that set forth company-specific, EU-compliant data-handling systems by which all entities of a global conglomerate are bound. This option allows a multinational corporation to freely transfer personal data relating to EU data subjects globally from one affiliate to another, provided the corporation adopts a uniform set of data protection rules applicable to all intra-group transfers of personal data originating from the EU. These binding privacy rules, once approved by the local EU member state, will be deemed to provide an adequate level of protection for data transferred from that particular EU country to any member of the corporate group in any non-EU country.

This BCR option is particularly suited for transfers of human resources data because it applies exclusively to intra-group transfers, and, unlike the EU Safe Harbor Accord, may also provide a truly “global solution” for large multinational companies with operations in a substantial number of countries. The corporate group must take steps to ensure that these rules are binding internally on a practical level. Notably, BCRs also must be structured in a way that would permit *judicial* enforcement in each EU country where they are effective – not just administrative enforcement by national data protection authorities.

The largest drawback to this option may have been the difficulty in gaining approval from individual member states. Since a company's BCRs had to be individually approved by each national data protection authority in which the company processed information or conducted business, requirements for approval can vary significantly by member state. With the increasing acceptance of the mutual recognition policy (see Question 307), BCRs may become less cumbersome.

Model Data Transfer Contracts (“Standard Contractual Clauses”): As a third option, multinational employers may be able to preserve their cross-border data flows through contractual agreements between entities sending and receiving personal data. In these contracts, the entity receiving the information agrees to abide by data protection provisions similar to the Safe Harbor Principles when processing transferred data.

The General DP Directive authorizes the EU Commission to approve transfers of personal data, including to third countries that fail to ensure an “adequate level of protection” if a controller establishes “sufficient safeguards” through “certain standard contractual clauses” consistent with a “commission’s decision.” For many organizations, however, this option may not be available with respect to human resources data because the European organization transmitting the information and the organization receiving the information must be legally independent entities in order to execute a binding, non-illusory contract.

Data Subject Consent: To be enforceable, consent must be unambiguous, informed and freely given by each concerned data subject. EU data authorities maintain that consent must specifically list the categories of data and the purposes for processing the data outside the EU.

301. What are standard contractual clauses?

These are contractual clauses adopted by the European Commission for ensuring adequate safeguards for personal data transferred from the EU to countries outside the EU. Member states are obliged to recognize that companies using such clauses in their contracts are offering “adequate protection” to personal data being transferred to countries outside the EU.

The standard contractual clauses contain a legally enforceable declaration whereby both the “data exporter” and the “data importer” agree to process the data in accordance with basic data protection rules and that individuals may enforce their rights under the contract.

Use of standard contractual clauses is voluntary. However, it can offer organizations a straightforward means of complying with their obligation to ensure “adequate protection” for personal data transferred to countries outside the EU that have not been recognized by the European Commission as providing adequate protection for such data.

302. What are the principles behind the standard contractual clauses?²⁷

The standard contractual clause principles reflect the provisions in the General DP Directive. Specifically:

- Personal data should be collected only for specified, explicit and legitimate purposes;
- The persons concerned should be informed about such purposes and the identity of the data controller;
- Any person concerned should have the right of access to his/her data and the opportunity to change or delete incorrect data; and
- If something goes wrong, appropriate remedies must be available to put things right, including compensation or damages through the competent courts.

The principal aim of the clauses is to ensure that these principles are applied when data is transferred outside the European Union.

303. How many sets of clauses are there?

There are two sets of standard contractual clauses, and both remain fully applicable. It is up to the operators to choose the one that best fits their needs. For example, the newest set (adopted by the Commission in 2004) does not cover data transfers to data processors in third countries. Lawyers and organizations with positive experiences with the 2001 standard contractual clauses may very well decide to continue using them.

A detailed explanation and information on the clauses can be found at:

http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

²⁷ Standard contractual clauses for the transfer of personal data to third countries – FAQ. MEMO/05/3. Brussels, January 7, 2005: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN>

304. Why are there two sets of standard contractual clauses and what are the main differences between them?

Due to demand from businesses for a wider choice of such clauses, the European Commission announced in May 2003 that it was open to providing organizations with more choices. The Commission accepted proposals by business representatives, provided this did not diminish the level of protection for data subjects.

The introduction of a second set of clauses allows companies to choose the set of clauses that best fits their business needs. Newer clauses such as those related to litigation, allocation of responsibilities or auditing requirements are more business-friendly. From the perspective of data protection and data subjects, both sets provide for a similar level of data protection. Individuals are similarly protected by both sets on the basis of the same “adequate” data protection standards and principles. Differences between both sets are mainly of a technical nature (for example, the conditions under which a data protection authority may carry out an audit in the data importer’s premises) or related to the differences in the system of liability.

Information on the adoption of the first set of standard contractual clauses can be found at:

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/851&format=HTML&aged=1&language=EN&guiLanguage=en>.

Information on the adoption of the second set of standard contractual clauses can be found at:

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/12&format=HTML&aged=0&language=EN&guiLanguage=en>.

305. Are the standard contractual clauses compulsory for companies interested in transferring data outside the European Union?²⁸

No, the standard contractual clauses are neither compulsory for businesses nor are they the only lawful way of transferring data to countries outside the European Union (EU).

First, organizations do not need contractual clauses if they want to transfer personal data to recipients in countries that have been recognized by the European Commission as providing adequate protection of data. This is the case for transfers to Argentina, Canada, Switzerland and the U.K. territories of Guernsey, Jersey and the Isle of Man. Neither are contractual clauses necessary to transfer data to U.S.-based organizations adhering to the Safe Harbor Privacy Principles issued by the U.S. Department of Commerce.

Second, even if the country of destination does not offer an adequate level of protection, data may be transferred if one of the exceptions in Article 26(1) applies.

Finally, national authorities may authorize, on a case-by-case basis, specific transfers to a country not classified as offering adequate protection where the exporter in the EU cites adequate data protection safeguards. This could be done, for example, by specific contractual arrangements between the exporter and the importer of data, subject to prior approval by national authorities.

306. Can companies implement the standard contractual clauses in a wider contract and add specific clauses?

The standard contractual clauses do not prejudice past or future contractual arrangements authorized by national data protection authorities pursuant to national legislation.

Parties are free to agree to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses approved by the European Commission or prejudice fundamental rights or freedoms of the data subjects. It is possible, for example, to include additional guarantees or procedural safeguards for individuals (e.g., online procedures or relevant provisions contained in a privacy policy).

Any such additional clauses that parties may decide to add are not covered by the third-party beneficiary rights. Therefore, they cannot be enforced by data subjects if they are not direct parties to the contract.

In all cases, the standard contractual clauses must be fully respected if they are to have the legal effect of providing an adequate safeguard for the transfer of personal data as required by the General DP Directive.

²⁸ Standard contractual clauses for the transfer of personal data to third countries – FAQ. MEMO/05/3. Brussels, January 7, 2005: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN>

307. How are Binding Corporate Rules used?

Binding Corporate Rules (BCRs) are used to allow multinational companies to transfer personal data lawfully from the European Economic Area (EEA) (i.e., the countries of the European Union, Iceland, Liechtenstein and Norway) to entities within their group but outside the EEA.

In the United Kingdom, using adequate BCRs ensures that a multinational organization will not breach the eighth data protection principle under the Data Protection Act 1998, which prohibits the transfer of personal data to a territory or country outside the EEA, unless that territory or country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Multinationals who seek to use BCRs to avoid liability for breach of the eighth principle must demonstrate that they have put in place adequate safeguards for the protection of personal data throughout the organization in line with the requirements (or “checklist”) of the Article 29 Data Protection Working Party paper on BCRs. Among other things, the checklist sets out the scope of the BCRs’ application, describing the data flows and the purposes of the data processing/transferring, and setting out a commitment on data quality, proportionality, transparency and a right to access.

In April 2005, the Working Party published a Working Document establishing a model checklist application for approval of BCRs. In June 2008, it followed up with consolidated guidance and further clarification, including FAQs and a framework for the structure of BCRs, incorporating all the necessary elements identified in previous guidance.

The benefits of BCRs

The key advantage of BCRs compared to other means of meeting the “adequate safeguard” criteria is that once they are in place, they operate as a framework for a range of intra-group transfers to meet the needs of a particular business. Provided the BCRs are drafted sufficiently widely, they should provide some flexibility in terms of accommodating changes in the company structure and alterations in the type of data flow without the need to notify any particular Data Protection Authority or seek fresh authorization.

This is an advantage over the use of model contract clauses, which are also used by multinationals as a way to ensure adequate safeguards. In multinational organizations with complex structures, hundreds of model contracts may be required to cover all the transfers between affiliates. Making sure the clauses in use are current and adequate can be a difficult and time-consuming process compared with the more straightforward ongoing obligation of a company that has received an authorization for its BCRs (i.e., monitoring compliance with BCRs and making sure the organization is operating within the scope of the authorization).

Another main advantage of BCRs is that they typically assist a multinational company with raising awareness of data protection throughout the organization. When putting together a BCR application, a company is required to consider the personal data that it transfers outside the EEA and how employees are made aware of the EU Data Protection Directive through training programs and other means.

Mutual Recognition Policy (MRP)

The MRP was agreed to by a number of European Data Protection Authorities (DPAs) in 2008. It involves one lead DPA assessing the adequacy of a company’s BCRs and the other data protection authorities in Europe accepting that assessment. This procedure is designed to avoid the applicant company having to approach each individual DPA separately and wait for a response from each.

The choice of a lead authority is dictated to a degree in that it generally depends on the location of the EU headquarters of the applicant company or the location within Europe of that part of the company best placed to take responsibility for global data protection compliance.

Prior to the MRP, if the lead authority was satisfied as to the adequacy of the safeguards put in place in the BCRs, that authority would circulate the draft BCRs to the other DPAs in Europe from which the applicant required authorization. The lead DPA would communicate any comments received to the applicant and would facilitate the authorization process.

The drawback to this process was that companies were reluctant to initiate an application due to the length of time that the authorization process would usually take. While the Information Commissioner’s Office (ICO) would always seek to deal with an application relatively quickly, the same could not be said for other European DPAs and the procedure could become unacceptably protracted.

Under the MRP, however, if the lead authority is satisfied that the BCRs have established adequate safeguards, other participating DPAs should have confidence in their decision and accept their findings without any further scrutiny or

comment. In a way, the MRP allows for “rubber stamping” of the lead DPA’s decision (which is measured against the EU Data Protection Directive (95/46/EC)), rather than undertaking a thorough review against national law.

Ultimately, the MRP helps to improve the BCR approval process by making it much simpler, less time-consuming, and more user-friendly for applicants.

308. Can U.S.-based companies that have not joined the Safe Harbor Accord use the relevant Safe Harbor rules under the contract?²⁹

Yes, provided they also apply the mandatory data protection principles in the appendix of Set I (applicable to all countries of destination) or similar restrictions reflected throughout Set II: the purpose limitation, restrictions on onward transfers and the right of access, rectification, deletion and objection.

If the data recipient is covered by a system providing adequate data protection such as the Safe Harbor, but the transfer concerns data not covered by their Safe Harbor commitments, the standard contract clauses can be used as a way of providing the necessary safeguards.

The Safe Harbor Agreement

309. What is the Safe Harbor Agreement?³⁰

Safe Harbor is unique to the United States. It is a voluntary self-certification system of compliance that ensures adequate protection for EU citizens’ personal information. The program’s data protection framework was negotiated by the U.S. Department of Commerce and the European Commission. U.S. companies that adhere to Safe Harbor requirements are deemed to have an “adequate level of protection” and thus are in compliance with the EU Directive 95/46/EC on the protection of personal data. Safe Harbor allows U.S. companies to receive personal data from Europe without experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities.

While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy, relying on a mix of legislation, regulation and self-regulation. Meanwhile, the EU relies on comprehensive legislation that requires, for example, creation of government data protection agencies, registration of databases with those agencies and, in some instances, prior approval before personal data processing may begin.

Because of these different approaches, the General DP Directive could have significantly hampered the ability of U.S. companies to engage in many transatlantic transactions. To bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed the Safe Harbor framework. It was approved by the EU in 2000.

Information on the adoption of the Safe Harbor Agreement by the European Commission can be found at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/00/865&format=HTML&aged=1&language=EN&guiLanguage=en>.

310. Are all U.S. organizations trading with EU countries required to register for Safe Harbor?

The decision is voluntary. U.S. companies that choose not to register for Safe Harbor status may instead have standard contractual clauses in place to cover the transfer of customer data. Refer to Question 300 for alternatives.

311. How does an organization join the Safe Harbor program?

Organizations that decide to participate in the Safe Harbor program must comply with its principles and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to self-certify annually, in writing, to the U.S. Department of Commerce that it agrees to adhere to the Safe Harbor requirements. These include elements such as

²⁹ Standard contractual clauses for the transfer of personal data to third countries – FAQ. MEMO/05/3. Brussels, January 7, 2005: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN>

³⁰ Safe Harbor Overview: http://www.export.gov/safeharbor/eg_main_018236.asp

notice, choice, access, and enforcement. The organization must also state in its published privacy policy statement that it adheres to the Safe Harbor Agreement. The U.S. Department of Commerce maintains a list of all organizations that file self-certification letters and makes both the list and the self-certification letters publicly available.

To qualify for the Safe Harbor program, an organization can (1) join a self-regulatory privacy program that adheres to the Safe Harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the Safe Harbor.

Safe Harbor Checklist for Joining: http://www.export.gov/safeharbor/eg_main_018274.asp

312. How do EU companies find out whether a U.S. organization is Safe Harbor registered?

The public list of Safe Harbor organizations is posted on the U.S. Department of Commerce's website. It contains the names of all U.S. companies that have self-certified to the framework. The list is updated regularly so that it is clear who is assured of Safe Harbor benefits.

U.S. Department of Commerce Safe Harbor list:

<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

313. What are the Safe Harbor Principles and what is required?

Organizations participating in Safe Harbor must comply with its seven principles. The Safe Harbor Agreement inherently involves compliance with the following criteria:

- **Notice.** Notice involves informing users, in clear and conspicuous language, of the purpose for which information about them is collected and used; the choice mechanism available for limiting use and transfer; the types of third parties to which data is transferred; and how to contact the organization for inquiries or complaints.
- **Choice.** An organization must offer individuals the opportunity to choose (i.e., opt out) whether and how personal information they provide is used or disclosed to third parties. An opt-in choice must be available for sensitive information.
- **Access.** Individuals must have reasonable access to personal information about them that an organization holds and must be able to correct, amend or delete that information, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
- **Onward Transfer.** An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected, or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the Safe Harbor Principles or that the third party provides at least the same level of privacy protection.
- **Security.** Organizations creating, maintaining, using, or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration, and destruction.
- **Enforcement.** A readily available and affordable independent recourse must exist for individuals (to whom the data relates) affected by an organization's noncompliance with the Safe Harbor Principles. For instance, an organization must have a dispute resolution system in place for investigating and resolving individual complaints. There also must be consequences for organizations that do not follow the principles.
- **Data integrity.** Personal information collected must be relevant to the purposes stated in the notice, and reasonable steps should be taken to ensure that the data is reliable, accurate, complete and current.

314. How is eligibility for Safe Harbor determined?

Any United States organization subject to the jurisdiction of the Federal Trade Commission (FTC), or U.S. air carriers and ticket agents subject to the jurisdiction of the U.S. Department of Transportation (DOT), may participate in the Safe Harbor program. Sectors that are not subject to the jurisdiction of either the FTC or DOT are not eligible for the Safe Harbor program.

315. How and where is the Safe Harbor program enforced?

Enforcement of the Safe Harbor program takes place in the United States in accordance with U.S. law and is carried out primarily by the private sector. Private sector self-regulation and enforcement is backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's Safe Harbor commitments the force of law vis-à-vis that organization.

Private Sector Enforcement: As part of their Safe Harbor obligations, organizations are required to have a dispute resolution system in place to investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the Safe Harbor Principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings of noncompliance and deletion of data in certain circumstances. They also may include suspension from membership in a privacy program (and thus, effectively, suspension from the Safe Harbor program) and injunctive orders.

Organizations can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities in Europe.

Government Enforcement: Depending on the industry sector, the FTC, comparable U.S. government agencies, and/or states may provide overarching government enforcement of the Safe Harbor Principles. Where a company relies in whole or in part on self-regulation in complying with the Safe Harbor Principles, its failure to comply with such self-regulation must be actionable under federal or state law prohibiting unfair and deceptive acts. Otherwise, it is not eligible to join the Safe Harbor program.

Under the FTC Act, for example, a company's failure to abide by commitments to implement Safe Harbor Principles might be considered deceptive and actionable by the FTC. This is the case even if a company adhering to the Safe Harbor Principles relies entirely on self-regulation to meet the requirements of the Safe Harbor "Enforcement" Principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to US\$12,000 per day for violations.

316. Approximately how many U.S. organizations have filed under Safe Harbor?

According to the U.S. Department of Commerce, as of February 2010, there are approximately 2,000 organizations that have notified the U.S. Department of Commerce that they adhere to the Safe Harbor framework.

317. What are the consequences of failing to comply with Safe Harbor requirements?

If an organization persistently fails to comply with the Safe Harbor requirements, it is no longer entitled to benefit from the agreement. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self-regulatory or government body, or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the U.S. Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act.

The U.S. Department of Commerce will indicate on the public list it maintains of organizations self-certifying adherence to the Safe Harbor requirements any notification it receives of persistent failure to comply. It also will make clear which organizations are assured, or are no longer assured, of Safe Harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for Safe Harbor must provide that body with full information about its prior participation in the Safe Harbor program.

The U.K. and the EU Data Protection Directives

Many U.K. companies are failing to comply with regulations governing the sending of unsolicited e-mails, according to a survey released by CDMS in January 2007. It claims that 31 percent of U.K. companies do not comply with the Privacy and Electronic Communications Regulations (Privacy Regulations 2003), which bans U.K. companies from spamming private individuals with electronic communications. Refer to the sidebar for recent U.K. information security breaches.

Recently, enforcers have been showing greater interest in punishing those who commit a breach with even heavier fines. In 2009, for example, the Financial Services Authority (FSA), which regulates the financial services sector in the United Kingdom (including how financial data is handled), imposed fines of £1.6 million, £850,000 and £700,000 on HSBC. Meanwhile, the Information Commissioner is pushing for FSA levels of fines for all data controllers who commit a breach, whether or not they are in the financial services sector.

The legislation requires that state companies should only send unsolicited sales messages via e-mail to non-customers if the customers have actively agreed that they want to receive such correspondence. In practice, this means that whenever someone's details are recorded – for instance, as part of a promotion or competition – they must be asked whether they want to receive subsequent sales marketing e-messages from that company or any other third party.

The U.K. Data Protection Act, which is also focused on the protection of personal data, contains rules around inappropriate unsolicited communications and direct marketing. The next section of this guide will examine the rights and obligations of businesses in relation to the U.K. Data Protection Act, the Freedom of Information Act 2000 and the Privacy and Electronic Communications Regulations 2003.

318. How has the United Kingdom addressed the EU Data Protection Directives?

The U.K. Data Protection Act came into force in March 2000 and is the statutory provision under which the U.K. implemented the General DP Directive. The DPA works in two ways.³¹ First, it states that anyone who processes personal information must comply with eight principles that are designed to ensure that personal information is:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Not kept for longer than necessary;
- Processed in line with an individual's rights;
- Secure; and
- Not transferred to other countries without adequate protection.

The second area covered by the DPA provides individuals with important rights, including the right to find out what personal information is held on computers and in most paper records.

Should individuals feel they are being denied access to personal information they are entitled to, or that their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office (ICO) for help. Complaints are usually handled informally, but if this is not possible, enforcement action can be taken.

The Privacy and Electronic Communications Regulations 2003, implemented into U.K. legislation from the E-Privacy Directive, sets rules for those who wish to send individuals electronic direct marketing. It covers unsolicited direct marketing messages sent by a range of electronic methods, including phone calls, faxes, e-mails and texts. Regardless of circumstances, those conducting direct marketing should always identify themselves, provide their contact information and suppress the details of those people who choose to opt out.

³¹ Data Protection Act, The Basics: http://www.ico.gov.uk/what_we_cover/data_protection/the_basics.aspx

319. Which authority in the United Kingdom administers compliance with the General DP Directive?

In the United Kingdom, the Information Commissioner's Office (ICO) is the independent supervisory authority set up in accordance with the General DP Directive. No other authority has responsibility for determining the way in which the DPA applies other than the courts. In this role, the ICO has a duty to exchange information with the other supervisory authorities in the European Economic Area (EEA) states as well as the European Commission.

Examples of U.K. data security breaches

December 2009

- Northern Ireland's Department of Finance and Personnel (DFP) admitted to the loss of personal data on 37,000 people. In total, 12 unencrypted laptops were stolen, two of which contained personal information. Details on the 37,000 people included payroll, employment and health data, although not all records contained these categories of information. Approximately 900 records contained bank details.

November 2009

- T-Mobile informed Britain's Information Commissioner's Office (ICO) of a data security breach in November 2009. An employee was to blame for stealing possibly millions of customer records and selling the data to competitors. The data included customers' contract renewal information, including customers' contract expiration dates. T-Mobile said the data was sold to "third parties."

January 2009

- Abertawe Bro Morgannwg University Trust and Tees, Esk and Wear Valleys Foundation Trust both had to sign formal undertakings to process personal information in line with the U.K. Data Protection Act. The decision follows losses of personal data by both National Health Service trusts. An unencrypted laptop containing the data of about 5,000 patients from Abertawe Bro Morgannwg was stolen. According to the Information Commissioner's Office (ICO), some of this data was sensitive.
- Tees, Esk and Wear Valleys Foundation Trust informed the ICO that it had lost a memory stick containing sensitive information on both patients and staff.

October 2008

- EDS lost a computer hard drive that contained sensitive data related to 100,000 Armed Forces personnel.

April 2008

- HSBC admitted to losing a disk containing details about 370,000 U.K. insurance customers.

January 2008

- The U.K. Ministry of Defence (MoD) lost a laptop containing details about 600,000 of its personnel.
- The National Health Service (NHS) admitted to losing a USB memory stick with more than 4,000 medical and personal records.

December 2007

- The Ministry of Justice lost four disks containing details about crime victims and witnesses.
- Her Majesty's Revenue and Customs (HMRC) admitted to losing the personal details of more than 6,500 people claiming pensions.

November 2007

- HMRC lost the personal details of 25 million child benefit recipients.

November 2006

- Laptop theft exposed Nationwide Building Society customers to the risk of financial crime.

Sources: www.bbc.co.uk, *Kable's Government Computing* at www.kable.co.uk, and www.publicservice.co.uk

The Commissioner also has a duty to help other supervisory authorities investigate complaints about the processing of personal data outside the United Kingdom where the data controller is U.K.-based and has specific duties in relation to certain decisions he/she may make about the international transfer of personal data.

320. What geographical areas are covered by the U.K. DPA?³²

U.K. enforcement authorities will regulate information society services provided from the United Kingdom, wherever in the EEA they are delivered. Similarly, information society services provided from elsewhere in the EEA will be regulated by the enforcement authorities in those member states. This means that U.K.-established service providers will need to comply with U.K. law when providing information society services to consumers elsewhere in the EEA.

Case Study: Companies that have been fined

In February 2007, the U.K. financial services regulator, the Financial Services Authority (FSA), fined the U.K.'s largest building society £980,000 following the theft of an employee's laptop. The laptop contained customer data relating to some of its 11 million account holders.

The FSA has criticized the Nationwide Building Society for failing to adequately address the risk that customer data might be lost or stolen. The laptop was stolen from the home of a Nationwide employee who reported the theft, but not the fact that the laptop contained such a significant amount of customer data.

The FSA indicated that Nationwide's risk assessment and security procedures were inadequate. The FSA specifically pointed to the fact that staff did not know what steps they were supposed to take in the event of such a breach. Policies were apparently inaccessible and staff members were not adequately trained. The fact that no action was taken in the first three weeks after the breach increased the opportunity for the information to be misused (although there was no evidence of its misuse). The FSA particularly noted that the failures occurred in an environment of heightened awareness of information security issues.

Of significance is the fact that the FSA, and not the U.K.'s data protection regulator, the ICO, has penalized Nationwide. Businesses regulated by the FSA, whose purview includes the supervision of systems and controls of the businesses it regulates, will need to reassess their data protection and data security risks urgently. The FSA rebuked Nationwide for not being prepared to deal with such an incident.

This is not the only recent example of a regulator other than a data protection authority (DPA) exercising jurisdiction over security breach issues in Europe. For instance, the Hellenic Authority for Communication Security and Privacy (ADAE) (Greece's privacy watchdog) fined Vodafone €76 million (US\$100 million) over a security breach and wiretapping incident at the time of the 2004 Athens Olympics.

Vodafone was ruled at fault for not preventing unknown hackers from subverting a legitimate surveillance system, supplied by Swedish firm Ericsson, to spy on Greek officials. The ADAE criticized Vodafone for obstructing its investigation by failing to own up about the surveillance system.

321. Why should businesses comply with the DPA?

It is a legal requirement to comply with the DPA. It should also be noted that other regulatory bodies are also entitled to monitor and enforce compliance with the DPA. (The following case study examples illustrate this point.)

It is crucial that data controllers comply with the DPA to avoid sanctions that can be imposed by the U.K. Information Commissioner's Office (ICO) and the courts. A recent significant development in the United Kingdom is the introduction of Section 144 of the Criminal Justice and Immigration Act 2008. It amends the DPA and empowers the ICO to impose substantial fines on organizations that deliberately or recklessly commit serious breaches.

³² Adapted from *A Guide For Business To The Electronic Commerce (EC Directive) Regulations 2002*. Department of Trade and Industry, July 2002.

Although the exact level of fine is yet to be set, the Ministry of Justice is currently consulting on the ICO being able to impose a maximum fine of £500,000 for serious breaches of the DPA.

The ICO can currently issue enforcement and “stop now” notices against organizations in breach of the DPA. However, this change represents a noteworthy shift in the law in the United Kingdom, as data controllers who breach data protection laws may face hefty fines if their breaches are deliberate or reckless and likely to cause substantial damage.

It also makes good business sense to comply with the DPA. For example:

- Sending out a mailing from incorrect or out-of-date records not only could annoy customers, but also waste time and money.
- Good information handling can improve a business’s reputation by increasing customer and employee confidence in an organization.
- Good information handling should also reduce the risk of complaints being made against the company. Every day, members of the public contact the ICO with inquiries about the way their information is handled. They can also ask the ICO to assess whether particular processing is likely or unlikely to comply with the DPA.
- If companies are not processing information in line with data protection requirements, and an individual suffers damage as a result, then that individual may seek compensation for the damage through the courts. This can result in negative publicity and legal costs.

322. What are companies’ obligations under the DPA?

Under the DPA, any individual is able to contact any U.K. business and request to know whether that business is processing personal data concerning them. A business processing any such information must give the individual a description of:

- The personal data of which that individual is the data subject;
- The purposes for which they are being or are to be processed; and
- The recipients or classes of recipients to whom they are or may be disclosed.

The business must inform the individual requesting the data of the information itself and the business’s source of that information.

All paper-based records that form part of a “relevant filing system” will be included within the ambit of a data subject’s access request. Businesses must ensure that the method of filing (structuring) makes for easy access to particular data.

Supply of personal data to the data subject must be in an intelligible form and should be accompanied with copies of all relevant files. Where the personal data is encoded by the data controller, the data subject should be given either a decoded version or the key.

323. What are the implications for data controllers with paper-based records?

Businesses with paper-based records should audit all such data to ensure that there is nothing within the files that the business would not wish the data subject to see. Appropriate action should be taken if the records are out-of-date or not required (for example, removing the paper from any structured file or, where appropriate, destroying it).

The audit of paper-based files should also include checks to ensure that the data is up-to-date and accurate and does not contain material that should not be seen by unauthorized employees or ex-employees.

324. What are the time periods for data controllers to respond to data requests?

Data controllers have to respond to a data subject’s access request within a period of 40 days. The period includes the day the request was received.

Where the data controller is a credit reference agency, the data controller is entitled to assume data requests by data subjects are limited to personal data relevant to their financial standing – unless a data subject specifies otherwise. The time limit for compliance is seven working days.

325. What are companies' rights under the DPA?

The data controller has the right to refuse supplying information unless it has received: (1) a request in writing, and (2) a fee for processing (except in prescribed cases).

The data controller is entitled to charge a fee for subject access, but it must not exceed the statutory maximum sum of £10. A higher fee of no more than £50 may be payable in the case of certain education and health records. The data controller is not obliged to comply with a request where it is uncertain about the identity of the person making the request.

The data controller may not comply with a request in situations where it cannot provide the information without disclosing information relating to another individual who can be identified from that information.

326. What are companies' obligations under the Privacy and Electronic Communications Regulations 2003?

- Unsolicited marketing transmitted by automated live phone calls must have the prior consent of the subscriber and must include the caller's identity.
- With non-automated, direct marketing phone calls, subscribers must be able to opt out. Those on the Telephone Preference Service (TPS) register should not receive any such calls unless they give their permission (Regulation 21).
- Organizations are not allowed to send unsolicited marketing faxes to individuals unless they have been requested. In addition, faxes may not be sent to individuals who or organizations that have registered their number with the Fax Preference Service (FPS). This is a list of telephone numbers of those who do not wish to receive unsolicited faxes. All organizations must screen their marketing fax lists against the FPS (Regulation 20).
- Unsolicited marketing material by electronic mail (this includes e-mail, text and picture messaging) should only be sent if the individual has consented to receive such correspondence, unless the individual's details were obtained in the context of a commercial relationship and the marketing is for similar products or services. The individual should always be given the opportunity to opt out in every message (Regulations 22 and 23).

The Privacy and Electronic Communication Regulations 2003 only apply to marketing e-mails sent from within the European Union (EU) and not material that comes from outside the EU. Currently, there is no specific legislation to cover e-mail sent to business addresses, although individuals should have the opportunity to opt out.

327. What are companies' rights under the Privacy and Electronic Communications Regulations 2003?

Companies or organizations, like individuals, have the right to refuse marketing by phone and fax. They can register with the Telephone Preference Service (TPS) if they do not want to receive unsolicited marketing calls. They can also register with the Fax Preference Service (FPS) if they do not want to receive unsolicited marketing faxes.

328. What are the consequences of noncompliance?

The Data Protection Act (DPA) has given the ICO extensive powers of enforcement that have been increased over time. For example, controllers could find these new powers used against them by disgruntled employees or customers who contact the ICO to allege an organization has breached the DPA's rules.

The ICO can serve a data controller with an "information notice" requiring the data controller to provide certain information within set time limits. Failure to comply with this notice or providing deliberately false information are criminal offenses. If the ICO concludes there has been a breach of the DPA, it may then serve a data controller with an "enforcement notice." This could force a data controller to cease processing personal data, or cease processing data in a particular way. Failure to comply with an enforcement notice is also a criminal offense.

Criminal liability does not apply only to the data controller. It is possible for officers of a company, such as its directors or managers, to be personally criminally liable if the offense has been committed with their consent, connivance or neglect. Employees may also incur criminal liability in certain limited circumstances if they disclose or obtain personal data without the authority of the data subject.

Although the commission of a criminal offense under the DPA will not result in a prison sentence, it will result in fines (which may be of an unlimited amount). Organizations also may be prevented from processing personal data as a result of an enforcement notice.

The Information Commissioner's Office (ICO) was recently granted new powers to fine up to £500,000 (\$800,000) for data security breaches and serious breaches of the UK Data Protection Act 1998. Statutory guidance about how the ICO will use the new power has already been approved by Justice Secretary Jack Straw and was approved by Parliament on January 12, 2010. The new power will now come into force from April 6, 2010. The Information Commissioner, Christopher Graham, will take a considered approach when issuing fines, with the £500,000 penalty being used in only the most serious circumstances. Moreover, factors such as an organization's financial resources, sector, size and the severity of the breach will be taken into account. A discount also has been agreed upon whereby the amount fined is reduced by 20 percent if it is paid within 28 days of the fine being issued.

329. What is notification?

Notification is the process by which a data controller informs the ICO of certain details about how it processes personal information. These details are used by the ICO to make an entry describing the processing in the register of data controllers that is available for public inspection. The ICO maintains this public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by the data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller. Each notification must include a general description of the processing of personal data being carried out. Notification does not exempt data controllers from compliance with other obligations in the DPA.

Further details for notification can be found at the ICO website:

http://www.ico.gov.uk/what_we_cover/data_protection/notification.aspx.

The ICO's Notification Handbook can be found at:

http://www.ico.gov.uk/upload/documents/notifications_handbook_html/index.html.

Once a company has registered with the ICO, it will be placed on the Data Protection Public Register. This can be found online at: <http://www.ico.gov.uk/ESDWebPages/search.asp>.

330. Why do data controllers have to notify?

The main purpose of notification and the public register is to promote openness in the use of personal information. Notification helps data controllers to be transparent about their processing activities, and also helps people understand how their personal information is being processed by data controllers. Under the Data Protection Act (DPA), every organization (data controller) that processes personal information (personal data) must notify the Information Commissioner's Office (ICO), unless it is exempt. Failure to notify is a criminal offense.

The obligation to notify arises out of Section 17 of the DPA, which stipulates that "personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Commissioner."

Data controllers exempt from notification must comply with the other provisions of the DPA. Data controllers exempt from notification may choose to notify voluntarily.

331. What information must be included in the notification?³³

The data controller will be asked for its name, address, contact information and company registration number (if relevant). The data controller will then be expected to make general statements about the types of processing undertaken and whether or not personal data is sent outside the European Economic Area (EEA).

The general statement includes information on the purposes of processing (e.g., for credit referencing, fundraising, trading in personal information), the data subjects whose data is being processed (e.g., staff, customers, agents), the classes of data processed (e.g. personal details, employment details, family and social circumstances), and to whom the data may be disclosed (e.g., prospective employers, financial institutions, the media). In each case, the data controller is given an opportunity to select from a list of available options.

³³ "The Ultimate Guide to the Data Protection Act 1998," Part II, Privacy & Data Protection journal: <http://privacydataprotection.co.uk/guide/part2/>

When data controllers are considering whether they will send personal data outside the EEA, they should keep in mind the need some businesses have to book foreign hotel rooms or airline tickets for their employees. They also should be aware that where personal data is available on the data controller's website, such availability will effectively be a transfer to all countries of the world. If data is to be sent outside the EEA, the notification must reflect this fact.

In addition, data controllers are expected to make a security statement. This consists of a series of questions to which the answer may be either "yes" or "no." There are no adverse consequences for answering with a "no." However, where data controllers find that their answers are in the negative, they should be aware their processing may breach the seventh Data Protection Principle.

If the data controller's processing changes after a notification is made, there is a duty to inform the ICO of this change as soon as possible. Data controllers should not wait until the expiry of their "notification year" to inform the ICO of the change. Notification is not a stand-alone process. Data controllers must also comply with the Data Protection Principles (notification does not exempt data controllers from compliance with other obligations in the Data Protection Act).

332. Are there any exemptions to notification?

Exemptions to notification are possible for:

- Some not-for-profit organizations
- Individuals who are processing personal data for personal, family or household affairs are exempt from notification and most of the other provisions of the DPA
- Data controllers who only process personal data for the maintenance of a public register
- Data controllers who only process personal data for any one or all of the following purposes for their own business:
 - Staff administration (including payroll)
 - Advertising, marketing and public relations (for their own business)
 - Accounts and records
 - National security
- Manual records that come within the scope of the DPA

333. How can companies find out if they are exempt?

The conditions required to be satisfied for each notification exemption are described in the ICO's *Notification Handbook*, which can be found at: http://www.ico.gov.uk/upload/documents/notifications_handbook_html/index.html

334. Are there any non-exempt areas?

Yes, there are non-exempt areas. These include:

- Private Investigation
- Health Administration and Services
- Policing
- Crime Prevention and Prosecution of Offenders
- Legal Services
- Debt Administration and Factoring
- Trading/Sharing in Personal Information
- Constituency Casework
- Education

If you process personal information for any of the above purposes, you are not exempt.

335. How can companies notify the ICO?

Data controllers are required to notify the ICO, which involves the controller's details being added to a public register of data controllers. The annual cost is £35.

There are three ways that companies can make an application to notify:

- **Internet:** Companies can complete a notification form online, print it out, and send it to the ICO with the notification fee or direct debit instruction. The web address is:
<https://forms.informationcommissioner.gov.uk/cgi-bin/dprproc?page=7.html>.
- **Post:** Alternatively, companies can complete a request for a notification form. The completed form can be faxed, posted or e-mailed (notification@ico.gsi.gov.uk) to the ICO, marked for the Notification Department's attention.
- **Telephone:** Companies also can call the notification helpline (01625 545740) between the hours of 9:00 a.m. and 5:00 p.m., Monday through Friday. The company will be asked to provide its name, address and contact details, and to specify the nature of its business. A notification form will be sent to be completed and returned by post.

336. What are the consequences of not notifying?

Processing data without notification, failing to renew a notification when companies are not exempt from notifying, or processing of a data type not reflected in the notification, are criminal offenses that are punishable by fines and can lead to prosecution by the ICO.

The ICO could take further enforcement action to make a company bring its processing into line with the principles. Failure to comply with an enforcement notice is also a criminal offense, punishable by a fine. The business's reputation and finances could also be affected, as individuals may seek compensation through the courts for any damage suffered.

Prosecutions by the ICO for breaching the notification and related requirements of the DPA take place in local magistrates' courts. For this reason, they tend to escape public attention. For example, between 1999 and 2000, 145 cases were prosecuted under the 1984 Act. In 130 of those cases, the result was a "guilty" verdict. (Examples of companies that were prosecuted can be found in the Appendices section of this guide.)

In summary, it is generally a criminal offense to:

- Process personal data without a register entry; and
- Fail to notify the ICO of changes to the registrable particulars.

In 2008, the ICO was granted new powers to levy fines against companies that breach U.K. data protection laws. Fine levels that can be levied have yet to be set by secondary legislation and so, for now, are potentially unlimited. Those persons/organizations processing data should take notice of this development and ensure they are not exposed to these new powers.

The Netherlands (NL) and the EU Data Protection Directives

The issues surrounding terrorism, fraud security of personal data, and privacy have all increased concern for the regulation of personal data protection. Changes in the healthcare system (the 2005 Health Care Insurance Act) have also focused yet more attention on the regulation and enforcement of data protection laws in the Netherlands. The Dutch Personal Data Protection Act (Wbp) implements the General DP Directive into Dutch law and is the main source of data protection legislation in the Netherlands. It was adopted by the Dutch Parliament in July 2000, and it entered into force in September 2001.

Note that Questions 337-351 are from http://www.dutchdpa.nl/Pages/en_ind_cbp.aspx.

337. What is the "Wet bescherming persoonsgegevens" (Wbp)?

Wbp is the Dutch Personal Data Protection Act. The most important rules for recording and using personal data have been set forth in the Wbp. This act was unanimously adopted by the Dutch Lower House on November 23, 1999, and accepted by the Dutch Upper House on July 3, 2000. The act came into force on September 1, 2001. The Wbp relates to every use ("processing") of personal data, from the collection of data up to and including its destruction. The Ministry of Justice has published guidelines for personal data processors.

338. Which authority in the Netherlands is responsible for data protection pursuant to the General DP Directive?

The Dutch DPA supervises compliance with acts that regulate the use of personal data. This means the Dutch DPA supervises compliance with, and application of, the Wbp and also the Wet politieregisters (Wpolr; Data Protection [Police Files] Act) and the Wet gemeentelijke basisadministratie (Wgba; Municipal Database [Personal Records] Act). The framework for performing this task has been set forth in the Wbp and other related legislation. In this context, the legislator has implemented Article 28 of the General DP Directive, which explicitly provides for the existence of such a supervisory authority and also provides that this authority should fulfill its task completely independently.

These tasks sometimes relate to obligations, but as a rule, they relate to powers. Subject to the law and the opinion of the court, the Dutch DPA is entitled to make decisions itself regarding execution of these powers. Other tasks, such as providing information and conducting studies of new developments, result from the general supervisory task. Also, in view of its independence, the Dutch DPA has considerable free rein to work out details of its tasks within the frameworks of the Wbp, set the necessary priorities, and decide where to place particular emphasis.

339. What are the duties of the Dutch DPA?

The duties of the Dutch DPA include:

- Making recommendations regarding legislation
- Testing codes of conduct
- Testing regulations
- Performing notification and preliminary examination
- Allowing exemption from the prohibition to process sensitive data
- Making recommendations regarding permits for transfers to third countries
- International affairs
- Mediation and handling of complaints
- Allowing official investigation
- Enforcement
- International tasks
- The publication of an annual public report explaining its work and findings

340. What guarantees apply regarding a proper performance of the tasks of the DPA?

In the execution of its powers, the Dutch DPA is bound by the standards set in the Algemene wet bestuursrecht (Awb; General Administrative Law Act). The Wbp also governs the tasks and powers of the Dutch DPA. As a national supervisory authority, the Dutch DPA is the successor of the former Registratiekamer. The Dutch DPA, as an administrative body, is also bound by the general principles of proper administration.

The Awb standards include:

- The possibility of objection to and appeal against Dutch DPA decisions to the administrative law court
- The possibility of submitting a complaint to the National Ombudsman
- That the Wet openbaarheid van bestuur (WOB; Freedom of Information Act) applies

341. What powers does the Dutch DPA have?

The Dutch DPA must be notified of the use of personal data (unless an exemption applies). Its powers include the supervision of compliance with the Wbp and enforcement of the Wbp (through the tasks listed above) and the authority to impose sanctions.

342. What are the individual's entitlements and company's obligations for individuals under the Wbp?

- **Entitlement to information.** A person whose personal data is processed must be able to find out what the information is and how it is processed. An organization or company must inform the individual about the goal regarding the retention of the data, and the name and address of whoever processes the personal data.
- **Entitlement to inspection.** A person whose personal data is processed can request an inspection of the personal data and the use of it by the organization or company.
- **Entitlement to correction.** A person whose personal data is incorrectly recorded has the right to have the data corrected.
- **Entitlement to petition.** A person whose personal data is processed has the right to petition for the use of the personal data.

343. When does the Wbp apply to the data processing of companies that operate internationally?

If the data controller is established in the Netherlands, the Wbp applies, regardless of where the data are processed or where the data subjects are. If the data controller is established in another European Union (EU) member state, the legislation of the other member state applies.

If a data controller has several branches in the EU, this party must ensure that each of the branches conforms to the rules of the country where the branch is located.

If the data controller is not established in the EU and processes personal data using means in the Netherlands, the Wbp also applies, unless these means are only used for the transfer of personal data. In these cases, the data controller must have a person who or body that represents it in the Netherlands.

344. When is the transfer of personal data to third countries (within and outside the EU) permitted?

Transfer of data within the European Union (EU)

The Wbp does not have any individual provisions governing data movements within the European Union, as the Wbp implements the European Directive for the Dutch jurisdiction. As stated above, this directive has two objectives:

- An equivalent protection of personal data; and
- Free movement of personal data within the EU.

Thus, the EU is one single jurisdiction with regard to protection of personal data. Once all member states have adapted their legislation to the directive, data movement from the Netherlands to another EU member state only has to conform to the Wbp's general requirements.

Transfer to countries outside the EU

The Wbp has specific provisions for the movement of data to countries outside the EU and "Third Countries." Third Countries are all countries outside the EU, with the exception of the countries of the European Economic Area (EEA). The countries of the EEA (Iceland, Liechtenstein and Norway) have undertaken to implement the directive in their own legislation.

Appropriate level of protection

The primary rule is that personal data may only be transferred to a Third Country if the general requirements of the Wbp have been conformed to and the Third Country ensures an adequate level of protection. For a number of countries, the European Commission has adopted decisions regarding the adequacy of the level of protection (for example, the Safe Harbor agreement for data transfers with the United States).

No adequate level of protection

If a Third Country does not provide an adequate level of protection, there are two possibilities for still being entitled to transfer data to these Third Countries:

- Transfer based on the exceptions mentioned in Article 77(1) Wbp.

- Transfer based on a permit of the Minister of Justice. Such a permit will be made subject to additional conditions that serve as a guarantee for the protection of personal data. To apply for the permit, a form must be used.

The granting of such a permit will be facilitated if the model contracts prepared by the European Commission are used for the transfer.

The Dutch DPA has various information materials regarding the transfer of personal data to Third Countries:

- **Fact sheet:** “Transfer to Third Countries,” which contains a brief summary.
- **The brochure:** “Third Countries – Transfers of Personal Data to Countries outside the European Union for a general orientation on requirements, exceptions and permits.”
- **For an extensive legal discussion of the subject:** “Policy Paper on Transfers of Personal Data to Third Countries in the Framework of the New Dutch Data Protection Act (Wbp).”

345. What are the penalties for data controllers if they breach the law?

Per the Wbp, the Data Protection Commission can apply “administrative measures of constraint” (Article 65) on data controllers who breach the law. Fines are also possible (Article 66, 75(1)) as is imprisonment if the offense was committed deliberately (Article 75(2)).

346. What is notification?

The Dutch DPA must be notified of all processing of personal data. The Dutch DPA keeps a public register of these notifications. However, a large number of socially well-known and accepted processing operations have been exempted from the notification obligation.

Detailed information on the Dutch notification process can be found at the following Dutch DPA website:

http://www.dutchdpa.nl/indexen/en_ind_melden.shtml

347. What information needs to be notified?

The Dutch DPA must be notified of the processing of personal data, unless specific processing has been exempted from the notification obligation.

348. Which personal data processing does not apply in the Wbp?

Without prejudice to Articles 17 to 22, the prohibition on processing personal data referred to in Article 16 does not apply where:

- This is carried out with the express consent of the data subject;
- The data has manifestly been made public by the data subject;
- This is necessary for the establishment, exercise or defense of a right in law;
- This is necessary to comply with an obligation of international public law; or where
- This is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy, and this is provided for by law or else the Data Protection Commission has granted an exemption. When granting an exemption, the Commission can impose rules and restrictions.

The prohibition on the processing of personal data referred to in Article 16 for the purpose of scientific research or statistics does not apply where:

- The research serves a public interest;
- The processing is necessary for the research or statistics concerned;
- It appears to be impossible or would involve a disproportionate effort to ask for express consent;
- Sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

Processing must be notified to the European Commission and shall be made by the minister concerned where the processing is provided for by law. The Data Protection Commission shall make the notification in the case that it has granted an exemption for processing.

349. How can a data processor determine if it is exempt?

In May 2001, the Exemption Decree was released by the Dutch DPA. This piece of legislation provides exemptions and simplifications to notification for certain categories of data. Detailed information about the exemptions can be found at: http://www.cbpweb.nl/indexen/ind_wetten_wbp_vrijstellingsbesluit.stm

350. How can the Dutch DPA be notified?

The Dutch DPA can be notified in three ways:

- Downloading the Wbp Notification Program (in Dutch)
- Requesting a copy of the disk with the Wbp Notification Program
- Requesting the special Wbp Notification Form

The Dutch DPA can only accept notifications that have been made in the prescribed way. The Dutch DPA will not accept notifications that have been sent on disk or by e-mail without a completed and signed authentication form. It will not accept notifications that are not in Dutch. All information must have been included on the disk or form itself. For this reason, no appendices (or reference to appendices) can be enclosed with the notification. In addition, organizations cannot send their “own” versions of the notification form.

More information about the notification process and conditions for accepting a notification can be found on the Wbp website: http://www.dutchdpa.nl/indexen/en_ind_melden.shtml

351. What are the consequences of not notifying?

The Dutch DPA must always be notified in advance of new processing and changes of existing processing. If an organization fails to notify the Dutch DPA of its data processing, the Dutch DPA can impose a fine. A fine can also be imposed if an organization has incorrectly or incompletely reported its data processing and/or if the organization fails to report changes.

Periodically, the Dutch DPA will carry out detailed checks on registered organizations from specific sectors.

Italy and the EU Data Protection Directives

The Italian Data Protection Directive (Personal Data Protection Code, Legislative Decree No. 196 of June 30, 2003) brings together all the various laws, codes and regulations relating to data protection since 1996. There are three key guiding principles behind the code:

- Simplification
- Harmonization
- Effectiveness

The Consolidated Text (Testo Unico) is concerned with the introduction of new guarantees for citizens, to the rationalization of existing norms, and replaces the parent law on the protection of the data, the No. 675 of 1996, as discussed below.

The code is divided into three parts. The first part sets out the general data protection principles that apply to all organizations. Part two provides additional measures that need to be undertaken by organizations in certain areas (for example, healthcare, telecommunications, banking and finance, or human resources). Part three relates to sanctions and remedies.

352. How has Italy addressed the EU Data Protection Directives?

The General DP Directive was first transposed in Italy by Act. No. 675 of December 31, 1996 (which has been effective since May 8, 1997), and then by the Legislative Decree No. 196 of June 30, 2003 (effective since January 1, 2004).

Directive 2002/58/CE was also transposed in Italy by the Legislative Decree No. 196.

353. Which authority in Italy is responsible for supervision, pursuant to the Data Protection Directives?

The Italian Data Protection Commission, known as Garante, is responsible for supervision, pursuant to the Data Protection Directives. It has a duty to act fully autonomously and independently in its decisions and assessments.

The Garante is a collegiate body composed of four members. Two members are elected by the Chamber of Deputies and two by the Senate through a specific voting procedure. The members consist of independent experts with proven experience in the field of law or computer science; both sectors shall be represented in the body at all times.

354. What powers does Garante have?

These are contained in Section 153 of the 2003 law. Section 154(1) outlines the tasks of Garante. Among the most important are:

- Verifying whether data processing operations are carried out in compliance with laws and regulations in force as well as with the relevant notification
- Verifying whether data processing operations are carried out in compliance with laws and regulations in force in cases of terminating processing operations
- Receiving reports and complaints, and taking steps as appropriate with regard to the complaints lodged by other data subjects or the associations representing them
- Ordering data controllers or processors to adopt such measures as are necessary or appropriate for the processing to comply with the provisions in force, per Section 143
- Prohibiting unlawful or unfair data processing operations, in whole or in part
- Raising public awareness of the legislation applying to personal data processing and the relevant purposes as well as of the data security measures

355. What are individuals' rights under the D.Lgs. 196/2003?

Individuals' rights are regulated by Section 7. A data subject has the right to obtain confirmation as to whether or not personal data concerning the subject exists (regardless of it being already recorded) and to communication of such data in an intelligible form.

The data subject has the right to be informed:

- Of the source of the personal data;
- Of the purposes and methods of the processing;
- Of the logic applied to the processing, if the latter is carried out with the help of electronic means;
- Of the identification data concerning the data controller, data processors and the representative designated as per Section 5(2); and
- Of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the state's territory, data processor(s) or person(s) in charge of the processing.

A data subject has the right to:

- Obtain confirmation as to whether or not personal data concerning him or her exists, regardless of that data already being recorded. Communication about such data also should be in an intelligible form;
- Obtain on legitimate grounds, information related to the processing of personal data concerning him or her;
- Erase, anonymize or block data that has been processed unlawfully, including data whose retention is unnecessary for the purposes for which it has been collected or subsequently processed; and to
- Obtain certification to the effect that the operations as per above have been notified and confirmation as to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

A data subject shall have the right to object, in whole or in part:

- On legitimate grounds, to the processing of personal data concerning him or her, even though it is relevant to the purpose of the collection; and
- To the processing of personal data concerning him or her, where it is carried out for the purpose of sending advertising materials or direct selling or for the performance of market or commercial communication surveys.

356. What are the implications for data controllers with paper-based records?

In the case of paper-based records, the “Titolare del Trattamento” must organize an efficient consultation system and, in particular, a rigorous physical security system that protects and monitors access to paper-based records.

357. What are companies’ obligations under the D.Lgs. 196/2003?

Companies’ obligations under the D.Lgs 196/2003 (Processing by Electronic Means) are:

- Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted:
 - Computerized authentication;
 - Implementation of authentication credentials management procedures;
 - Use of an authorization system;
 - Regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintaining electronic means;
 - Protection of electronic means and data against unlawful data processing operations, unauthorized access and specific software;
 - Implementation of procedures for safekeeping backup copies and restoring data and system availability;
 - Maintenance of an up-to-date security policy document; and
 - Implementation of encryption techniques or identification codes for specific processing.
- In the case of a higher-risk category of paper-based data, the company must place the information into archives and establish:
 - A rigorous access system; and
 - An appropriate physical security system for the archives.

358. What are the consequences of noncompliance?

Noncompliance can be a civil or criminal offense and the consequences can be detrimental for organizations.³⁴ Further details are set out below:

Civil offense

- **Art. 161 Providing no or inadequate information to data subjects.**
Breaches in providing no or inadequate information to data subjects are punishable by a fine consisting in payment of between €3,000 and €18,000. If sensitive or judicial data are involved or the processing entails specific risks indicated in Section 17, or if more serious harm is caused to one or more data subjects, the fine can be increased to €5,000 to €30,000. The amount may be increased by up to three times if it is found to be ineffective on account of the offender’s economic status.
- **Art. 163 Submitting no or an incomplete notification.**
Failure of timely submission of notification or provision of incomplete information in a notification is punishable by a fine consisting of between €10,000 and €50,000. There is also the additional sanction of an injunction/order, in whole or in part, and publication of the offense in one or more daily newspapers.

³⁴ Personal Data Protection Code, Legislative Decree No. 196 of June 30, 2003, p. 100 –103.

- **Art. 164 Failure to provide information or produce documents to the Garante.**
Failure to provide the information or failure to produce the documents requested by the Garante in relation to Sections 150(2) and 157 is punishable by a fine consisting of between €4,000 and €24,000.

Criminal offense

- **Art. 167 Unlawful data processing.**
 - 1) Any person who, for himself or another, or with intent to cause harm to another, processes personal data in breach of Sections 18, 19, 23, 123, 126, 129 and 130 is punishable by imprisonment for between six and 18 months or, if the offense consists of data communication or dissemination, by imprisonment for between six and 24 months.
 - 2) Any person who, for himself or another, or with intent to cause harm to another, processes personal data in breach of Sections 17, 20, 21, 22(8) and (11), 25, 26, 27, and 45 is punishable by imprisonment for between 1 and 3 years if harm is caused.
- **Art. 168 Untrue declarations and notifications submitted to the Garante.**
Whoever declares or attests to untrue information or circumstances, or else submits forged records or documents, in connection either with the notification referred to in Section 37 or with communications, records, documents or statements that are submitted or made, as the case may be, in a proceeding before the Garante and/or in the course of inquiries, is punishable by imprisonment for between six months and 36 months.
- **Art. 169 Security measures.**
 - 1) Whoever fails to adopt the minimum measures referred to in Section 33 can be punished by detention for up to two years or else by a fine of between €10,000 and €50,000.
 - 2) A time limit can be set for the offender to comply with the requirements referred to above. The time limit must not exceed the time span technically required; however, it may be extended in especially complex cases or because of objective difficulties in complying, but it shall not be longer than six months.

Within 60 days of the expiry of the above deadline, the offender shall be permitted by the Garante to pay one-fourth of the highest fine that can be imposed in connection with the offense, on condition that the relevant requirements have been complied with. Compliance and performance of the above mentioned payment shall extinguish the offense.

- **Art. 170 Failure to comply with provisions issued by the Garante.**
Failure to comply with a provision issued by the Garante pursuant to Sections 26(2), 90, 150(1) and (2) and 143(1), letter c), shall be punished by imprisonment for between three months and two years.

The economic sanctions can be tremendous because they are calculated on the value of the organization. In some cases, the Garante can forbid the use of the organization's data to do business.

359. What is notification?

Notification is a declaration by the data controller informing the Garante that it wishes to process personal data. The areas of processing covered are:

- Genetic data, biometric data, or other data disclosing geographic location of individuals or objects;
- Data disclosing a person's health and sex life;
- Data disclosing political, philosophical, religious or trade-union character;
- Data indicating an individual's consumption patterns and/or choices;
- Sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys; and
- Data in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

Notification must be submitted by means of a single form and must include information on cross-border data flows, if it is part of the data processing.

Once a company has notified, the Garante enters the notified information into a publicly available register:

<https://web.garanteprivacy.it/rgt/NotificaEsplora.php>

Further information can be obtained from the Garante website:

<http://www.garanteprivacy.it/garante/doc.jsp?ID=488582>

360. What information needs to be notified?

When notifying, data controllers (Titolare del trattamento) must provide the following:

- Information to identify the data controller and, where appropriate, his or her representative, as well as the arrangements to identify the data processor if the latter has been appointed;
- The purpose(s) of the processing;
- A description of the category/categories of data subject and the data or data categories related to the said category/categories of data subject;
- The data recipients or the categories of data recipient;
- Data transfers to third countries, where envisaged; and
- A general description that shall allow assessment beforehand as to whether the measures adopted to ensure security of the processing are adequate.

A new notification is only required prior to termination of processing operations or in connection with the modification of any of the items to be specified in the notification.

361. Are there any exemptions to notification?

Yes. Notification that is related to higher-risk categories of data, as indicated in Article 37. For example, notification shall not be required if it concerns an activity carried out by general practitioners and/or freely chosen pediatricians.

362. How can I find out if I am exempt?

Categories in Article 37 are exempt from notifying.

363. How can notification be performed?

Notification can be performed online via the Garante website: <https://web.garanteprivacy.it/rgt/>

364. What are the consequences of not notifying?

If an organization fails to notify or notifies behind schedule, the Garante can impose a fine. The value can be between €10,000 and €50,000. The organization's failure to notify can also be published in the press, which can give rise to negative publicity.

False or inaccurate notification is a crime and is punishable by imprisonment, from six months to three years.

365. What is the Security Policy Document (Documento Programmatico sulla Sicurezza)?

The Legislative Decree stipulates that by March 31 of each year, the controller of processing operations concerning sensitive and/or judicial data must draw up a security policy document containing appropriate information with regard to:

- The list of processing operations concerning personal data;
- The distribution of tasks and responsibilities among the departments/divisions in charge of processing data;
- An analysis of the risks applying to the data;
- The measures to be taken to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purposes of keeping and accessing such data;
- A description of the criteria and mechanisms to restore data availability following destruction and/or damage;
- A schedule of training activities concerning the persons in charge of the processing. Areas of training must include risks applying to the data, measures available to prevent harmful events, the most important features of personal data protection legislation in connection with relevant activities, the resulting liability, and the arrangements to get updated information on minimum security measures adopted by the data controller;
- A description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalized in accordance with the Code; and

- The personal data disclosing health and sex life. The recommendation is to implement encryption or keep this type of data separate from other personal data concerning the same data subject.

Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures, the data controller is required to supply a written description of the activities performed and seek certification that they are compliant with certain provisions.

Additionally, the fact that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit.

Appendix A

U.S. Legal and Regulatory Resource Summary

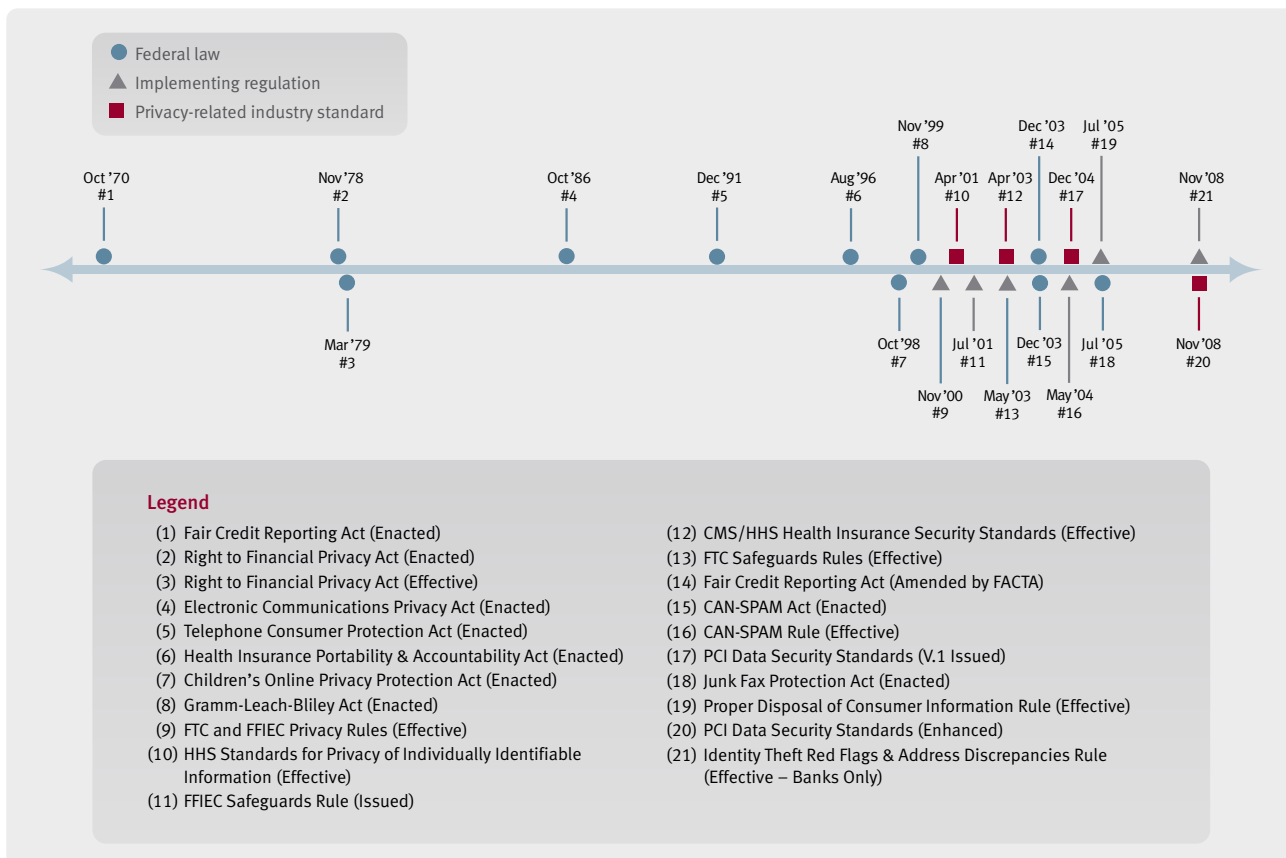
Legal and Regulatory Releases			
Gramm-Leach-Bliley Act (GLBA)			
11/12/1999	Federal Law	Gramm-Leach-Bliley Act	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf
5/24/2000	Final Rule	FTC: Financial Privacy Rule	http://ftc.gov/os/2000/05/65fr33645.pdf
5/23/2002	Final Rule	FTC: Safeguards Rule	http://www.ftc.gov/os/2002/05/67fr36585.pdf
12/2001	Regulatory Guidance	FTC: “Frequently Asked Questions for the Privacy Regulation”	http://ftc.gov/privacy/glbact/glb-faq.htm
2/1/2001	Regulatory Guidance	FFIEC: “Interagency Guidelines Establishing Standards for Safeguarding Customer Information”	http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf
5/9/2001	Regulatory Guidance	FDIC: “Guidance on Identity Theft and Pretext Calling”	http://www.fdic.gov/news/news/financial/2001/fil0139a.html
7/2002	Regulatory Guidance	FTC: “How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act: A Guide for Small Businesses”	http://ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm
4/1/2005	Regulatory Guidance	FFIEC: “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”	http://www.fdic.gov/news/news/financial/2005/fil2705.html
10/2005	Regulatory Guidance	FFIEC: “Authentication in an Internet Banking Environment” (i.e., the “Multifactor Rules”)	http://www.ffiec.gov/pdf/authentication_guidance.pdf
Health Insurance Portability and Accountability Act (HIPAA)			
8/21/1996	Federal Law	Health Insurance Portability & Accountability Act	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ191.104.pdf
2/20/2003	Final Rule	CMS/HHS: Health Insurance Reform: Security Standards	http://aspe.hhs.gov/admsimp/FINAL/FR03-8334.pdf
12/28/2000	Final Rule	Standards for Privacy of Individually Identifiable Health Information	http://aspe.hhs.gov/admsimp/final/pvcguide1.htm
12/15/2008	Regulatory Guidance	HHS: Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information	http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf
3/31/2009	Regulatory Guidance	HHS/HISPC: “Health Information Security and Privacy Collaboration: Provider Education Toolkit Final Report and Implementation Guide”	http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_872353_0_0_18/PET_3_Final_Rpt_with_all_app.pdf

Legal and Regulatory Releases <i>(continued)</i>			
Fair Credit Reporting Act (FCRA) and Fair and Accurate Transactions Act (FACTA)			
12/4/2003	Federal Law	Fair and Accurate Credit Transactions Act	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf
6/3/2008	Federal Law	Fair Credit Reporting Act, Amended	http://www.ftc.gov/os/statutes/fcradoc.pdf
11/9/2007	Final Rule	Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule	http://files.ots.treas.gov/481019.pdf
7/1/2005	Final Rule	Proper Disposal of Consumer Information under the Fair and Accurate Credit Transactions Act	http://www.fdic.gov/news/news/press/2004/pr12804a.html
10/24/2008	Regulatory Bulletin	OTS: Information Technology Risks and Controls and Fair Credit Reporting Act	http://files.ots.treas.gov/74843.pdf
1997-2001	Regulatory Guidance	FTC FCRA Staff Opinion Letters	http://www.ftc.gov/os/statutes/fcra/index.shtm
Children's Online Privacy Protection Act (COPPA)			
10/21/1998	Federal Law	Children's Online Privacy Protection Act	http://www.ftc.gov/ogc/coppa1.htm
11/3/1999	Final Rule	Children's Online Privacy Protection Rule; Final Rule	http://www.ftc.gov/os/1999/10/64fr59888.pdf
12/2006	Regulatory Guidance	FTC: How to Comply With The Children's Online Privacy Protection Rule	http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm
–	Regulatory Guidance	FTC: You, Your Privacy Policy and COPPA	http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus51.pdf
Right to Financial Privacy Act (RTFPA)			
1978	Federal Law	Right to Financial Privacy Act	http://www4.law.cornell.edu/uscode/12/ch35.html
12/1999	Examination Handbook	OTS: Right to Financial Privacy Act	http://files.ots.treas.gov/422240.pdf
Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)			
12/16/2003	Federal Law	CAN-SPAM Act	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf
2004	Final Rule	CAN-SPAM Rule	http://www.ftc.gov/os/2005/01/050112canspamfrn.pdf
Electronic Communications Privacy Act (ECPA)			
10/21/1986	Federal Law	Electronic Communications Privacy Act (ECPA)	http://www.usiia.org/legis/ecpa.html
Junk Fax Protection Act (JFPA)			
7/9/2005	Federal Law	Junk Fax Protection Act	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ021.109.pdf
4/6/2006	Regulatory Guidance	Miscellaneous Rules	http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-06-42A1.pdf
10/1/2003	Final Rule	Miscellaneous Rules Relating to Common Carriers	http://edocket.access.gpo.gov/cfr_2003/octqtr/47cfr64.1200.htm

Privacy-Related Industry Standards			
The Information and Communications Technology (ICT) Industry's Global Network Initiative			
–	Initiative Principles	Global Network Initiative Principles	http://www.globalnetworkinitiative.org/principles/index.php
–	Implementation Guidelines	Global Network Initiative Implementation Guidelines	http://www.globalnetworkinitiative.org/implementationguidelines/index.php
–	Accountability Framework	Global Network Initiative Governance, Accountability & Learning Framework	http://www.globalnetworkinitiative.org/governanceframework/index.php
Payment Card Industry (PCI) Data Security Standards			
10/1/2008	Security Standards	PCI Data Security Standard	https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
2008	Reference Guide	PCI Quick Reference Guide	https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
National Automated Clearinghouse Association (NACHA) Guidelines			
2010	Operating Guidelines	ACH Operating Rules and Guidelines (purchase required)	https://nacha.org/member-apps/index.cfm?action=store.main

Appendix B

A Timeline of Pertinent Laws and Regulations



Appendix C

United Kingdom: Case Studies of Companies Breaking the Data Protection Act 1998³⁵

Example 1

Since April 2005, the Information Commissioner's Office (ICO) has received various complaints regarding the inappropriate disposal of confidential personal data at different branches of a leading mobile phone retailer. Following an investigation into incidents that occurred at branches in Coventry and Swindon, the company agreed to sign an undertaking to ensure their future compliance with the Seventh Data Protection Principle.

Example 2

The ICO received complaints from individuals regarding the processing of personal data by a leading online retailer. Individuals continued receiving marketing material, despite having given notice in writing that the data controller cease processing their personal data for the purpose of direct marketing.

The ICO ordered the retailer to remove all of the affected individuals' data from all company databases thereby ensuring the individuals will not receive any future marketing material.

Example 3

The ICO ruled that a large mobile telephone operator breached the Data Protection Act's security requirements following a complaint about the way in which it processed personal information, in particular, the way in which new members of staff were allowed to share usernames and passwords when accessing the company's IT system. Following its investigation, the ICO found the company was not keeping its customers' personal information secure and therefore was in breach of the DPA. The ICO required the company to enter into undertakings to cease breaching the Act, failure to comply with which could lead to a large fine.

Example 4

In February 2010, the Information Commissioner's Office (ICO) found the Labour Party in breach of the Privacy and Electronic Communications Regulations (PECR) for making unsolicited automated marketing calls without consent to almost half a million people. David Smith, deputy commissioner at the ICO, warned that automated calls can cause annoyance and disruption, which is why it is so important for organizations making such calls to gain the consent of individuals. The enforcement notice was served and requires the Labour Party to ensure no further automated direct marketing calls are made without consent. Failure to comply with the enforcement notice would be a criminal offense and could lead to prosecution.

Appendix D

United Kingdom: Case Studies of Companies Breaking the Privacy and Electronic Communications Regulations³⁶

A leading mobile telephone retailer signed a legal undertaking in agreement with the ICO to stop making unsolicited direct marketing calls to individuals without their consent. This legally binding agreement followed a number of complaints about breaches of the regulations made to the ICO and the Telephone Preference Service (TPS). The agreement means that the retailer concerned cannot make calls for direct marketing purposes to people registered with the TPS or to individuals who have specifically told the company that they do not wish to receive direct marketing calls, and breaches of the agreement will lead to a substantial fine.

³⁵ http://www.ico.gov.uk/complaints/data_protection.aspx

³⁶ http://www.ico.gov.uk/complaints/privacy_and_electronic_communications.aspx

Appendix E

Italy: Case Study on Security Measures in Processing Telephone Traffic Data³⁷

A complaint was lodged against a leading telecom company in Italy, with regard to Sections 7 (Right to Access Personal Data and Other Rights), 8 (Exercise of Rights), and 145 (Right to make Complaints) of the Personal Data Protection Code (legislative decree no. 196/2003) and with regard to the considerations made by the Office as submitted by the Secretary General pursuant to Section 15 (Damage Caused on Account of the Processing) of the Garante's Rules of Procedure (no. 1/2000).

The complainant objected to the unlawful "dissemination" of data, which allegedly was "only available" to the said company, and the complainant wanted to know "the grounds" on which the data had been processed.

Considering that his request had not been granted, the complainant lodged a complaint with the Garante (under Section 145 et seq. of the DP Code) including a detailed list of requests pursuant to Section 7 of the DP Code.

In submissions presented on March 22, 2006, the complainant considered the replies as unsatisfactory and expressed several doubts as to data security; furthermore, he requested the Garante "to take such measures as may be appropriate in order to prevent similar events from occurring in future."

The telecom company declared that it could not "establish whether some IT staff might have carried out unlawful operations" because "the system is only configured in such a manner as to record accesses in log files rather than to track the detailed operations performed."

Based on the above premises, the Garante ruled that:

- In order to safeguard the data subject's rights, computerized solutions should be adopted without delay, in any case by no later than 120 days from the date of the decision, with a view to ensuring control of the activities carried out by any and all persons in charge of the processing – irrespective of their capacity, tasks and scope of activity – with regard to any and all types of processing carried out.
- The respondent must confirm, both to the data subject and to the Garante, that the measures set out in the above provision had been implemented in full.
- The company was required to pay €500 to the complainant by way of compensation.

Appendix F

References – European Union Privacy and Information Security Laws and Regulations

Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, European Commission report, Tender No. XV/97/18/D.

"Coming to America: The EU privacy directive," Lamphere, Patrick, *Computerworld*, June 14, 2007.

"Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC," *Official Journal of the European Communities*, 2002/16/EC.

"Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," European Commission press release, available at http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm.

³⁷ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1303462>

Commission Staff Working Document on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC), European Commission report, 2006.

Data Protection Act 1998 (1998 Chapter 29), U.K. Parliament, available at the Office of Public Sector Information website, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF>.

“Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),” *Official Journal of the European Union*, L 201, July 2002.

“Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,” *Official Journal of the European Union*, L105, March 15, 2006.

“Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” *Official Journal of the European Union*, L 281, pages 31-50, November 23, 1995.

Dutch Personal Data Protection Act 2000 or “Wbp” (Wet Bescherming Persoonsgegevens), http://www.dutchdpa.nl/Pages/en_ind_wetten_wbp_wbp.aspx

European Data Privacy Law and Online Business, Kuner, Christopher, Oxford University Press, 2003, citing Bundesverfassungsgericht [BVerfGE] [Federal Constitution Court], November 15, 1983, 65 Entscheidungen des Bundesverwaltungsgerichts [BVerfGE] 1 (F.R.G.).

The EU Data Protection Directive: Implications for the U.S. Privacy Debate, U.S. House of Representatives, Committee on Energy and Commerce, March 8, 2001, Serial No. 107_19, <http://ftp.resource.org/gpo.gov/hearings/107h/71497.pdf>.

Freedom of Information Act 2000 (2002 Chapter 36), U.K. Parliament, available at the Office of Public Sector Information website, <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm>.

“General information on new Italian data protection code 2007,” available at http://www.dataprotection.it/codice_privacy_english.htm.

A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI2002/2013), Department of Trade and Industry, July 31, 2002, available at <http://www.berr.gov.uk/files/file14635.pdf>.

Handbook on Cost-Effective Compliance with Directive 95/46/EC, Masons Solicitors and Privy Council Agents, published for the European Commission, August 1998.

Italian Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003.

Negotiating Privacy: The European Union, The United States, and Personal Data Protection, Heisenberg, Dorothee, Lynne Rienner Publishers, Inc., Boulder, Colo., 2005, pages 27-28.

The Privacy and Electronic Communications (EC Directive) Regulations 2003, U.K. Parliament, available at <http://www.opsi.gov.uk/si/si2003/20032426.htm>.

“Protection of individuals and other subjects with regard to the processing of personal data,” ACT No. 675 of 31.12.1996, Italian privacy law, <http://www.privacy.it/legge675encoord.html>.

“Safe Harbor Agreement – Boon or Bane?,” Kierkegaard, Sylvia Mercado, *Shidler Journal of Law, Commerce and Technology*, August 2, 2005, <http://www.lctjournal.washington.edu/vol1/a010Kierkegaard.html>.

“Standard contractual clauses for the transfer of personal data to third countries – Frequently asked questions,” Europa website, press release, January 7, 2005, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN>.

“The Ultimate Guide to the Data Protection Act 1998 (Parts I, II and III),” *Privacy & Data Protection Journal*, available at <http://privacydataprotection.co.uk/guide/>.

Appendix G

Terms and Definitions and Useful Websites

Terms and Definitions:

The following key definitions have been taken from Directives 95/46/EC, 2002/21/EC and 2006/24/EC and are used throughout this document. This is designed to act as a quick reference point when interpreting data protection jargon used in the various Directives.

- **Controller** – The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
- **Data Subject** – A living individual who is the subject of the data.
- **EEA State** – A state that is a contracting party to the Agreement on the European Economic Area signed at Oporto on May 2, 1992, as adjusted by the Protocol signed at Brussels on March 17, 1993.
- **Electronic mail** – Any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
- **Personal data** – Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
- **Processing of personal data ("Processing")** – Any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Processor** – A natural or legal person, public authority, agency or any other body who/that processes personal data on behalf of the controller.
- **Recipient** – In relation to any personal data, any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
- **Registered company** – A company registered under the enactments relating to companies for the time being in force in the United Kingdom.
- **Telephone service** – Calls (including voice, voice mail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multimedia services (including short message services, enhanced media services and multimedia services).
- **The data subject's consent** – Any freely given, specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

Useful Websites:

<http://www.protiviti.com>

<http://www.pillsburylaw.com>

<http://europa.eu>

<http://www.ico.gov.uk/>

<http://www.opsi.gov.uk/>

<http://www.dutchdpa.nl>

<http://www.cbpweb.nl>

<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp>

<http://www.privireal.org>

http://www.export.gov/safeharbor/eg_main_018236.asp

<http://www.access.gpo.gov/congress/house>

<http://banking.senate.gov/conf/>

<http://epic.org/privacy/globa/>

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm>

<http://www.ftc.gov/privacy/glbact/glb-faq.htm>

<http://www.hipaa.org/>

<http://cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm>

<http://www.hipaa.com/>

About Pillsbury Winthrop Shaw Pittman LLP

Pillsbury Winthrop Shaw Pittman LLP is a full-service law firm with market-leading strengths in the energy, financial services, real estate and technology sectors. With offices in the world's major financial and technology centers, we counsel clients on all aspects of global transactions and litigation. Our multidisciplinary teams allow us to anticipate trends and offer a 360-degree perspective on complex business and legal issues—helping clients take greater advantage of opportunities and better mitigate risk.

The firm's multidisciplinary Privacy & Data Protection practice provides counsel and services on the gamut of legal issues and litigation relating to privacy, data collection, information security and information management. Two of the firm's attorneys, Deborah Thoren-Peden and Wayne Matus, are recognized in Chambers USA 2009 and Chambers Global 2010 as leading attorneys in privacy and e-discovery, respectively. Pillsbury's privacy team drafts, implements and revises privacy and security policies related to customer, employee and vendor information; provides training on policies and procedures; prepares appropriate contract provisions; handles a broad range of privacy-related disputes and litigation; and assists companies both when a security breach occurs and to prepare for handling such an occurrence. When clients are engaged in marketing, outsourcing, data modeling or joint ventures, the team guides them on the privacy issues these activities may raise.

The team also works in close collaboration with related firm practices such as Communications, where we counsel on privacy issues arising under the Communications Act and subject to the jurisdiction of the Federal Communication Commission, and Global Sourcing, where we advise on restrictions and requirements for outsourcing arrangements with domestic and international service providers.

Pillsbury continuously provides our clients and other members of the privacy industry with complimentary updates in the form of client alerts and articles, as well as speaking engagements and comments to the media on new privacy developments. In 2009, the practice's attorneys spoke at a number of important conferences including the Information Systems Audit and Control Association (ISACA); the Association of Corporate Counsel (ACC); the Knowledge Congress; and the California Bankers Association. We have also prepared numerous client alerts and written articles and chapters in privacy treatises.

For more information about Pillsbury's Privacy & Data Protection practice, please go to www.pillsburylaw.com or contact:

Rafi Azim-Khan
+44.20.7847.9519
rafi.azim-khan@pillsburylaw.com

Gerry Hinkley
+415.983.1135
gerry.hinkley@pillsburylaw.com

Wayne Matus
+212.858.1774
wayne.matus@pillsburylaw.com

Catherine Meyer
+213.488.7362
catherine.meyer@pillsburylaw.com

John Nicholson
+202.663.8269
john.nicholson@pillsburylaw.com

Deborah Thoren-Peden
+213.488.7320
deborah.thoren-peden@pillsburylaw.com

About Protiviti Inc.

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East. Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Protiviti's Privacy and Security Management Practice

Protiviti's Privacy and Security Management practice includes compliance executives, former regulators and information technology specialists with deep credentials in developing, implementing, and executing world-class Privacy programs for companies of all sizes across industries and geographies. We understand the unique challenges associated with aligning business objectives, compliance requirements, and technology constraints, and offer proven, practical insights to manage these challenges.

Our services include:

- Designing and executing global Data Privacy Improvement Programs including Data Privacy inventories, Privacy impact and risk assessments and Privacy compliance audits
- Developing Information Security risk assessment frameworks, written compliance programs, Board reporting strategies and templates, and independent testing plans
- Assisting companies to implement new or revised Privacy requirements imposed by law or regulation, including U.S. requirements, EU Data Protection Directives, and establishing Safe Harbor and/or Binding Corporate Rules (BCR) programs
- Enhancing the effectiveness of identity management approaches to improve privileged access to information
- Helping clients improve the effectiveness of their Data Governance programs by assessing the lifecycle of data management, covering areas as data usage, quality, integrity, Privacy, and effective records and discovery risk management
- Developing breach response programs, and assisting in the investigation and resolution of actual Security and Privacy breaches
- Executing Security and Privacy vulnerability assessments to test controls in place to maintain compliance, and improve the strength of the technology infrastructures supporting the enterprise

For more information about Protiviti's Privacy and Security Management capabilities, please contact:

Carol Beaumier
+212.603.8337
carol.beaumier@protiviti.com

Mike Brauneis
+312.476.6327
michael.brauneis@protiviti.com

Hernan Gabrieli
+39.02.6550.6301
hernan.gabrieli@protiviti.com

Ryan Rubin
+44.207.389.0436
ryan.rubin@protiviti.com

Cal Slep
+203.905.2926
cal.slep@protiviti.com



ATTORNEY ADVERTISING. Results depend on a number of factors unique to each matter. Prior results do not guarantee a similar outcome.

www.pillsburylaw.com

© 2010 Pillsbury Winthrop Shaw Pittman LLP.
All rights reserved.



Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

www.protiviti.com

© 2010 Protiviti Inc.
An Equal Opportunity Employer.