

This questionnaire was developed by a bank member of the ABI for use in preparing an inventory of all their practices involving the use of customer information. The inventory is one of the first steps in confirming that all relevant activities are brought into compliance with the Gramm-Leach-Bliley Act. The Questionnaire will need to be tailored to each company's situation, but might serve as a helpful starting place. This material is provided solely for educational and informational purposes with no warranties, expressed or implied, being made regarding the information.

CUSTOMER PRIVACY QUESTIONNAIRE

- A “customer” refers to consumers and sole proprietorships (not corporate or small businesses), and includes prospects, declined applicants, current customers, and former customers.
- A “customer” can be located in the U.S. or can be international.
- The term “customer privacy” refers to how “Bank” protects the privacy of its customers.
- The term “business unit” refers to your organizational unit within your line of business, which may be an affiliate, a division, a delivery channel, or other discrete entity.
- The term “third party” refers to a “non-Bank” entity. There are two types of third parties; those to which you outsource certain business functions (“outsourcing third parties”) and those with whom you have affinity, co-branded, joint venture or other marketing-related relationships (“unaffiliated third parties”).

Notice and Awareness

1. Does your business unit inform customers about its customer information practices?
 - 1a If yes, do you accomplish this through your FCRA Notice? Please specify the frequency with which this notice occurs.
 - 1b Do you accomplish this through a privacy policy or practice statement separate from the FCRA notice? If yes, please attach. Please specify the frequency with which this notice occurs.
 - 1c Is the privacy policy or practice statement conspicuous and readily available to customers? Where does this notice appear?
2. Do you inform customers of how your business unit collects personal data? If so, how?
 - 2a If yes, are customers notified prior to initial collection?
3. Do you inform customers of how your business unit intends to use the information collected? If so, how?

- 3a If yes, are customers notified prior to initial collection?
4. Do you inform customers that their information may be shared with third parties? If so, how?
5. Do you educate consumers about privacy in other ways than described above? (e.g., FAQs document, hyper-link to external privacy resources) If yes, how and where? If yes, please attach.

Collecting Customer Information

1. How do you collect information from your customers (applications, Internet, telephone, etc.)? Please describe.
7. What type of information do you collect from your customers? Please describe.
8. Do you purchase or collect information about your customers from outside sources (e.g., outside lists, marketing companies, external databases)?
- 8a If yes, please specify the names of these outside data sources.
- 8b. Describe the type of information collected.
1. Do you purchase or collect information about prospects (potential customers) from outside sources (e.g., outside lists, marketing companies, external databases)?
- 9a If yes, please specify the names of these outside data sources.
- 9b Describe the type of information collected.
10. Do you collect information about customers from other “Bank” business units? If so, please describe.
- 10a If yes, please specify the names of these business units.
- 10b Describe the type of information collected.

Using Customer Information within the Corporation

11. Do you provide customer information to other “Bank” business units for purposes other than a customer-initiated transaction (e.g., marketing or cross-selling)? If yes, please identify which business units.
- 11a If yes, please describe what type of data is shared.
- 11b Please describe how this data is shared.

12. Can customers opt-out of data sharing across the corporation for purposes other than a customer-initiated transaction?
 - 12a If yes, are these opt-outs provided prior to sharing? If so, how?
 - 12b Can customers opt-out of marketing based upon type of channel (i.e., email, phone, direct mail)? If yes, please describe.
 - 12c Are customers informed of the consequences of opting out of collection, use or marketing of personal data? (e.g., no notice of special offers or relationship pricing)
13. Do you provide your customers the ability to opt out of the marketing of other products and services offered by your business units? If yes, where and when does this opt-out choice take place?
14. Is there an authorization process through which other business units must go in order to access and use your customer information? If yes, please describe.
15. Do requests for customer lists go through a list management organization? If yes, please describe where this list management function resides and who is the point of contact.
 - 15a Does list management filter out customers who have opted out via FCRA (Fair Credit Reporting Act)? If yes, describe where this filter file is located and who is responsible for managing it.
 - 15b Does list management filter out customers who do not want to receive marketing solicitations? If yes, describe where this filter file is located and who is responsible for managing it.
 - 15c Does list management filter out customers from sold banking centers according to regulations? If yes, describe where this filter file is located and who is responsible for managing it.
 - 15d Does list management filter out customers whose names appear on the Direct Mail Association (DMA) 'do not call' list? If yes, describe where this filter file is located and who is responsible for managing it.
 - 15e Are the filter files described above combined, or exist separately?
 - 15f Are there any other filter files not mentioned here? If yes, please describe.
 - 15g Are the filter files refreshed periodically? If yes, how often?
16. Are certain customers provided (or need to be provided) higher levels of privacy protection based upon business needs or regulatory requirements? If yes, please describe.

17. Are there certain business units with which you do not want to share customer information? If so, please describe.
18. Do you use information about other business units' customers for marketing purposes? If yes, describe how you obtain the customer lists.
19. Are formal agreements established with other "Bank" business units for customer data sharing? If so, please attach.
21. For the information you retain on former (attritted) customers, do you use this data?
 - 21a. If yes, this is former customer information used for marketing purposes such as reacquisition? Please describe.
 - 21b. Is this former customer information provided to other "Bank" business units? Please describe.
 - 21c. For how long is information about former customers retained?
22. Do you maintain information on declined applicants?
 - 22a. If yes, is this declined applicant information used for marketing a different product offering? Please describe.
 - 22c. For how long is information about declined applicants retained?

Is customer information being shared between your business unit and third parties? If yes, please continue here. If not, skip to the next section. Note that there are two types of third parties—those to which you outsource certain business functions ("outsourcing third parties") and those with whom you have affinity, co-branded, joint venture or other marketing-related relationships (unaffiliated third parties)

23. Do you outsource certain business functions to third parties which have access to your customer data (e.g., data processing, billing, customer service)? If yes, please identify each outsourcing third party and type of data shared.
 - 23a. If yes, do the contracts established with outsourcing third parties address the use of customer information? Please describe.
 - 23b. Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
24. Do you use third parties to sell your business unit's products (e.g., mortgage brokers, online business partners)? If yes, please describe.

- 24a If yes, are there contract provisions which address the use of customer information? Please describe.
- 24b Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
25. Do you securitize any of your products?
- 25a If yes, are there contract provisions which address the use of customer information? Please describe.
- 25b Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
26. Do you sell the servicing of any of your products?
- 26a. If yes, are there contract provisions which address the use of customer information? Please describe.
- 26b Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
27. Do you share customer information with other types of unaffiliated third parties? (e.g., marketing, independent user)? If yes, please identify each third party and type of data shared.
- 27a If yes, are there contract provisions which address the use of customer information? Please describe.
- 27b Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
28. Do you receive income for customer information provided to unaffiliated third parties?
- 28a. If yes, what is the nature of the exchange? Please describe.
- 28b What type of information is provided (e.g., name, address, transaction history, social security #)?
- 28c What are the names of these unaffiliated third parties?
- 28d Are there other controls or practices (beyond the contract) to protect customer information? If yes, please describe.
29. Are you aware of any third parties which share your customer information with other third parties? If yes, please describe.

30. Is there an authorization process to sign on additional unaffiliated third parties? If yes, please describe.
31. Are third parties periodically audited or reviewed to validate their continued compliance with customer privacy and security requirements? If yes, how?
32. Are customers allowed to opt-out of the sharing of their information with unaffiliated third parties?
 - 32a If yes, are these opt-outs provided prior to sharing? Please describe.
 - 32b Are customers informed of the consequences (e.g., no special offers, reduced Internet functionality) of opting out of information sharing with unaffiliated third parties?
27. Do you acquire customers in bulk from other corporations (e.g., loan portfolio purchases, securitizations, mergers and acquisitions)? If so, please describe.
 - 33a if yes, do you respect their previous choices for opt-out (if any)? If so, how?
 - 33b Do you provide these customers with a new opt-out opportunity? If yes, please describe.

Customer Access and Correction

34. Do you allow customers access to the customer-supplied data that is maintained by the corporation (e.g., privacy preferences, email address)?
 - 34a If yes, please describe how customers access this data.
 - 34b Please describe what type of data customers can view.
35. Can customers submit changes to customer-supplied information? If yes, how?
36. Do you allow customers access to the corporation-generated data about the customer (e.g., customer segment, credit score)?
 - 36a If yes, please describe how customers access this data
 - 36b Please describe what type of data customers can view
37. Can customers submit changes to corporation-generated information? If yes, how?
38. How quickly do you respond to correct inaccurate or updated information?
39. Are confirmations given to the customer that their corrections have been effected? If yes, how?

40. Are changes communicated to other business units with which the customer has a relationship? If yes, describe.

Information Security

41. Do you have controls to protect customers' social security numbers beyond those controls for other types of customer data? If yes, please describe.
42. How do you use social security numbers to identify customers within your business unit?
42. Do you provide customers' social security numbers to unaffiliated third parties? If yes, please describe.
43. Do you have formal procedures for authenticating customers via the telephone or by fax? If yes, please describe.
44. Do you have formal procedures for authenticating customers via the Internet? If yes, please describe.
45. Do you have formal procedures for authenticating customers in person at a banking center? If yes, please describe.
46. Do you have formal procedures for authenticating customers through the mail? If yes, please describe.
47. Do you have formal procedures to assist customers who have forgotten their password, PIN or other identification? If yes, please describe.

Accountability

48. Is there a single point of contact in your business unit responsible for addressing customer information practices? If so, please indicate this person's name and phone number.
49. Do you inform customers how to contact your business unit or the corporation regarding privacy questions or concerns? If so, please indicate how.
50. Is there an escalation process to address privacy concerns, if necessary? If yes, please explain.
51. Are you aware of any loss of business due to your customers' concerns over privacy? If so please describe.
52. Do you measure or track customer privacy complaints or concerns? If yes, please describe.
53. Are your customers' information practices audited or reviewed?

55a If yes, is this review related to FCRA? If yes, please describe.

55b Are there other (non-FCRA) reviews performed? If yes, please describe.

Do you have any customers located outside the US? If yes, continue here. If not, skip this section.

54. Do you have customers located in the European Union (EU)? If so, approximately how many?

55. Do you have customers located in non-EU countries? If so, approximately how many? Please list major countries.

56. Does your business unit handle customer privacy issues differently for customers located outside the US? Please describe.

57. Has your business unit specifically addressed the European Union Privacy Directive? If yes, please describe.

58. Are there planned initiatives within your business unit for 2000 to establish a presence outside the US? If yes, please describe.

Does your business unit collect information from customers or visitors through the Internet? If yes, please continue. If no, skip to the next section.

59. Do you collect customer data or manage transactions through the "Bank".com web site? If yes, please describe.

60. Do you collect customer information or manage transactions through your business unit's web site? If yes, please provide the web address in the comments section.

63a If yes, please describe the type of information collected.

63b If yes, does that web site have a posted privacy policy? Please attach.

63c If yes, does that web site use cookies to track visitors? If so, please describe.

61. Do you collect customer data through a relationship with a "non-Bank" or shared web site (e.g., joint marketing effort with a strategic partner such as Excite or AOL)? Please provide the web address in the comments field.