

About This Manual

Protecting Customer Privacy: Management Process from Policies to Quality Control Checklists provides an in-depth discussion and review of customer data security and data privacy, including related data management techniques, decision processes, data analysis tools, data reporting or MIS, sample data privacy policies and privacy notices with supporting procedures, and current and emerging issues. The information is based on the laws and regulations, including Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act of 1999 (GLB Act), and the Privacy of Consumer Financial Information regulation (released by The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (the Board), the Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS) on May 9, 2000).

You and your financial institution's management team may use the assembly of insights, narrative guidelines, and actual tools to evaluate the various data privacy and data security options available. The accompanying CD contains significant historic as well as recent issuances regarding privacy from the federal financial institution regulatory agencies.

Addressing Customer Data Privacy and Data Security Management Considerations

The manual focuses on basic challenges for today's financial institution management:

- How does bank management identify, analyze, and determine what viable data privacy and data security management options exist?
- If data resources are available and an interested third party wants to purchase a database, how does an institution's management team determine whether those resources or opportunities are appropriate for the institution?
- How does senior management pursue a data privacy approach, from the initial idea through requesting customer input on data sharing?
- How would the board of directors provide direction through a flexible approach to corporate governance to address all types of data privacy and data security management issues that might arise?

These challenges are further complicated by the very nature of business conducted by financial institutions every day. Public trust and confidence in the institutions that handle personal and business financial transactions must be without exception or concern. Absent that trust and confidence, the basic foundation of the United States financial system weakens. Recognizing this, regulatory agencies have developed specific issuances to address data privacy and security management areas. These include data security, minimum data standards, data reporting controls, sharing data with affiliated vs. nonaffiliated third parties, and vendor support.

The Gramm-Leach-Bliley Act

Section 501, Protection of Nonpublic Personal Information, subtitle A, title V – Privacy, of the GLB Act focuses specifically on financial institution safeguards with respect to appropriate standards for the administration, technical protection, and security of customer data. Congress, in passing the act, set out specific language stating that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of a customer’s nonpublic personal information. Accordingly, each financial institution regulatory agency was charged with the responsibility to develop guidelines to accomplish the following tasks:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of records or information, which could result in substantial harm or inconvenience to any customer

The Privacy of Consumer Financial Information Regulation

The regulatory agencies focused first on the issuance of privacy regulations and the opt-out requirements of information sharing. With the release on May 9, 2000, of the Privacy of Consumer Financial Information regulation, the OCC, the Board, FDIC, and OTS presented guidelines on security and confidentiality of customer information. The purpose of the rule as stated in the regulation is as follows:

... the rule is intended to require a financial institution to provide notice to customers about its privacy policies and practices; to describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and to provide a method for consumers to prevent a financial institution from disclosing that information to certain nonaffiliated third parties by “opting out” of that disclosure, subject to various exceptions as stated in the rule.

This joint rule became effective November 13, 2000. However, compliance was optional until July 1, 2001. Examiners, at that point, started to test and evaluate procedures, processes, and internal controls to protect customer data. This manual advocates a posturing of proactive approaches for these regulatory requirements.

In early 2001, the joint agencies provided further guidance regarding expectations for the creation, implementation, and maintenance of a comprehensive information security program. The issuances provided guidelines and detailed specific information security focus points.

Designing and Implementing an Organizational Approach to Protecting Customer Data

Protecting Customer Privacy provides a starting point to assess the areas of risk regarding customer data privacy and data security. The risk assessment worksheets included in this manual make it possible for you to assess what your bank already has in place regarding customer information databases, data controls, data procedures, and the types of data security and privacy policies. After gathering this information, you can then use the manual’s step-by-step approach to design and implement an organizational plan.

The manual also contains questionnaires and worksheets to aid you in documenting the assessment process and the development initiatives. Sample monitoring procedures will help you assess performance, and the sample internal audit procedures and sample examination procedures provide a final performance assessment.

A Perspective on How to Deal With Security Flaws

Today, banks, customers, and companies use websites as an integral part of their daily life. They conduct both personal and job-related business on websites. And they make purchases online, using sensitive credit card information.

But are these transactions secure? Companies have implemented protocols such as SSL and many hire security experts to conduct vulnerability assessments. However, security is still a major concern for institutions who offer secure websites and for potential users. Surveys continue to be conducted to assess customer satisfaction with regard to online banking.

A recent industry study determined that current security measures that are being employed appear to secure online banking to a much greater degree than just a few years ago and that a major problem is in educating potential customers on the security and convenience of online banking.

Other industry studies analyzed financial institutions for design flaws that would prevent websites from secure usage. A number of U.S. financial institution websites were used for this analysis.

- *Problems relating to break-in-the-chain of trust problems.* A secure website is considered to be the root of trust for the user. However, the break-in-the-chain can happen when websites forward users to new pages that have different domains without notifying the user from a secure page. The user does not have any way of knowing whether the new page is truly secure.
- *Problems when attempting to secure login options on insecure pages.* Some websites will present a login form that will then forward to a secure page. However, the initial forms do not come from a secure page. Users are particularly at risk because when faced with these situations, they have no way of knowing if their usernames and passwords have been sent to a hacker site.
- *Problems faced with contact information/security advice found on an insecure page.* Some websites have hosted their security recommendations, contact information, and various other sensitive information about their site and company on insecure pages. This puts the website in a very vulnerable situation, as an attacker could forge the insecure page and present different recommendations and contact information.
- *Problems relating to user ids and passwords.* The study found instances where websites would allow customers to use short passwords and user IDs. Some sites would allow customers to use short passwords or require e-mail addresses for user names. There were instances where there was no stated policy on allowed passwords or companies permitted weak passwords.
- *Problems when using the e-mail system to send security sensitive information insecurely.* Financial institutions or companies should be extremely cognizant of e-mailing sensitive

information. Studies revealed that some sites offered to send statement and passwords through e-mail but not very many people have secure e-mail.

Overall, the consensus revealed that most financial websites are not adequately protected against secure usability design flaws. Many sites continue to provide login windows on non-SSL pages.

Current Impact of Identity Theft — Insights

Based on a report by the Federal Trade Commission (FTC) entitled “Identity Theft Tops FTC Complaint List Again,” dated February 14, 2008, identity theft was the number one source of consumer fraud complaints for the seventh year in a row. According to the agency’s yearly report on fraud complaints for 2007, of 813,899 total complaints received in 2007, 32 percent were related to identity theft.

According to the FTC, total consumer fraud losses totaled \$1.2 billion, with the average monetary loss for an individual at \$349. Credit card fraud was the most common form of reported identity theft (23 percent), followed by utilities fraud (18 percent) employment fraud (14 percent), and bank fraud (13 percent).

The top form of credit card fraud was opening a fraudulent new account (14.2 percent), followed by fraud on an existing account (9.4 percent).

The FTC compiled fraud data from consumer complaints in all 50 states and the District of Columbia, and identified the 50 metropolitan areas with the highest incidence of fraud and identity theft. The metropolitan areas with the highest per capita rates of reported consumer fraud complaints were Albany-Lebanon, Oregon, Greeley, Colorado and Napa, California.

Costs, Types of Fraud Vary Widely

Based on a survey from the Federal Trade Commission (FTC) prepared by Synovate in November 2007, 8.3 million Americans, or nearly 4 percent of the population, were victims of identity theft in 2005.

Of those victims, 3.2 million experienced fraud or misuse of their existing credit card accounts, 3.3 million suffered fraud or theft from non-credit card accounts, and 1.8 million were defrauded when thieves stole their personal information to open new accounts in the victims’ names, known as “new account fraud.”

The survey also looked at the costs of identity theft. The survey revealed that the value of goods stolen and the costs of recovering from these thefts varied according to the type of fraud involved. Where the identity theft was limited to the misuse of existing accounts, the average loss was less than \$500, although much higher losses were reported in some cases.

However, when the type of fraud was extended to “new account fraud,” the losses were much higher. Specifically, the median value of goods and services obtained by the thieves was \$1,350. Among new account fraud victims, 10 percent reported losses of \$15,000 or more in goods and services, with the top 5 percent of victims reporting losses of \$30,000 or more in goods and services.

Recovering from new account fraud was more time consuming and costly to the victims as well. Ten percent of all victims reported out-of-pocket expenses of \$1,200 or more. But for new account fraud, the

top 10 percent of the victims incurred expenses of at least \$3,000, and the top 5 percent incurred expenses of at least \$5,000.

Thirty-seven percent of victims reported experiencing problems such as harassment by debt collectors, being unable to get loans, having their utilities cut off, being subject to a criminal investigation or civil suit, being arrested, and having difficulties obtaining or accessing bank accounts.

In cases of new account fraud, victims were more than twice as likely to report having one or more of these types of problems than when thieves misused only existing accounts, according to the survey.

The survey also found that 84 percent of the identity theft victims polled did not know the thief, contradicting other studies that claimed the majority of identity theft crimes were committed by friends or relatives.

Sixteen percent claimed some personal knowledge of the thief in their case, with 6 percent of victims reporting a family member or relative as the thief, 8 percent claiming a friend or neighbor, and 2 percent claiming a colleague on the job was the thief. The victims who reported knowing the identity of the thief were also more likely to identify how the information was taken than those who did not.

Thirty-eight percent of the victims polled said the most trying part of the experience was dealing with authorities or agencies in order to get the effects of the theft reversed, including dealing with credit bureaus and lenders, and replacing credit cards and existing accounts.

The study was conducted through interviews with 4,917 people between March 27 and June 11, 2006.

Companies Likely Involved In Identity Theft

While consumers are constantly told to avoid identity theft, there has been limited information about the companies most likely to be involved in identity theft, which can make it hard to take effective preventive action.

A new report from the Berkeley Center for Law and Technology finds that the world's largest banks and telecommunications companies are most frequently the companies that fall for identity theft crimes. These incidents make life miserable for victimized consumers, according to data collected from the FTC.

The Report, entitled "Measuring Identity Theft at Top Banks," represents a compilation of 88,000 complaints filed with the FTC over three months in 2006. It shows that major banks and telecommunications companies accounted for a much larger portion of the filed complaints than other industries, and that telecommunications companies lacked a standard of measuring the complaints.

According to author Chris Hoofnagle, the report was designed to provide consumers and regulators "objective tools" to compare banks and utilities based on how they handle security and incidents of fraud and theft.

Hoofnagle's findings revealed that Bank of America ranked highest of all the companies studied, with an average of 1,117 incidents over the three-month period. Next was AT&T with 763 incidents, followed by Sprint Nextel with 698. Rounding out the top five were JP Morgan Chase (including Chase and Bank One) with 613 cases and Capital One with 442.

The Organization of the Manual

Protecting Customer Privacy: Management Process from Policies to Quality Control Checklists is organized into four parts and appendixes and has an accompanying CD. The information is divided among the following parts:

- Part I: Legal Background for Use of Confidential Information
- Part II: Establishing an Information Privacy Policy
- Part III: Data Privacy Relating to Specific Operations
- Part IV: Review and Performance Measurement

The appendixes contain a glossary, quick reference guides, and the final Privacy of Consumer Financial Information regulation, released May 9, 2000. The accompanying CD contains the significant regulatory issuances from previous years that pertain to privacy. You can quickly access any issuance in full by clicking on its title on the CD's opening page.

PART I: LEGAL BACKGROUND FOR USE OF CONFIDENTIAL INFORMATION

Chapter 1: Legal and Regulatory Requirements

This chapter focuses on the numerous laws and regulations and describes how each applies to data security and data privacy. Because the terms used to describe privacy for regulatory purposes must be understood before implementing the regulation, this chapter defines the critical terms, such as customer, consumer, nonpublic information, and publicly available information. In reviewing data privacy and security management techniques, this chapter outlines objectives of managing data access and ensuring data privacy. Plus, the chapter details the Federal Trade Commission's principles on fair information practices, and the FDIC's contribution concerning privacy notices. This chapter also describes components of data privacy and data security implementation timeline. The chapter concludes with sample privacy principles.

Chapter 2: Marketing vs. Privacy: How Customer Data May Be Used

This chapter focuses on collecting data and how that data may be used. Marketing to current customers and an explanation of unacceptable practices precedes a discussion of general marketing to consumers. The potential problem areas, such as telemarketing and its restrictions, are also discussed. The banks must be diligent in maintaining their information systems regarding the customer opt-out provision. This chapter explains when consumers/customers can opt-out, the exceptions to opt-out notice requirements, and opt-out operational issues. The chapter concludes with helpful reference of data elements, in-depth flowcharts to walk you through the process of deciding how data may be used, a regulatory checklist, and samples of different types of opt-out notices.

Chapter 3: Legal Restrictions on Data Sharing

Privacy is not a new concept. Over a number of years, various laws have been enacted, and numerous regulations have been implemented. This chapter reviews relevant components of two statutes: Fair Credit Reporting Act and the GLB Act. The chapter also notes the relevance of the Health Insurance Portability and Accountability Act of 1996 in terms of dealing with privacy issues. The focus of the chapter is the Privacy of Consumer Financial Information regulation, which is analyzed section by section, with examples demonstrating the regulation's guidance. The chapter concludes with a data checklist regarding protecting customer data for each act and a checklist to determine if your bank can take advantage of the reduced regulatory requirements.

PART II: ESTABLISHING AN INFORMATION PRIVACY POLICY

Chapter 4: Drafting a Corporate Policy and Customer Policy Statement

Many organizations have been challenged to address data privacy on an organizational basis for the first time. While certain departments or areas have had data privacy and security issues to consider for years, privacy has become a corporatewide issue. This chapter describes the general objectives and specific components of a privacy policy and helps you assess your bank's existing policies in relation to a privacy policy. A checklist is provided to assist you in determining what components should be in this type of policy. Sample corporate customer data protection/privacy policy, customer data protection/privacy notice, and statement of privacy principals are provided as exhibits. For certain institutions, a number of the privacy regulation requirements, e.g., opt-out notice, do not apply. A separate policy has been designed as a sample for community banks.

Chapter 5: Implementing the Policy

Developing and implementing procedures to address data privacy and data security are the primary focuses of this chapter. There is a guide to control points and risk areas to aid in the initial effort to design, develop, and implement procedures. An emphasis is placed on using a checks-and-balances methodology to assist in monitoring data privacy and data security. Sample procedures, which parallel both sample policies in the previous chapter, are provided with supporting exhibits including privacy coordinator job description, customer data privacy risk assessment worksheets, risk assessment analysis support documents, and a profile of state privacy laws.

Chapter 6: Data Security Protection

Developing an appropriate security environment for data privacy and data security is the focus of this chapter. The components of strong information and data protection practices are offered along with specific suggestions for establishing data security levels, creating "walls" (both physical and electronic) to protect data from outsiders, and protecting your bank against cyber-terrorism. The chapter also provides in-depth control review checklists concerning various customer data sources and the techniques used to protect the data and ensure data privacy.

Chapter 7: Training: A Necessary Process

For your bank to be in compliance with the regulation, your employees must be trained in all areas of the law. This chapter helps you identify needs and develop a training program. Sample training materials are provided.

PART III: DATA PRIVACY RELATING TO SPECIFIC OPERATIONS

Chapter 8: Online and Internet Banking

Electronic banking is one of the major areas of concern regarding protecting customer privacy. In this chapter, information is provided about different types of Web sites, the collection of customer data from such sites, the importance of disclosure statements to customers, the use of information, and related concerns pertaining to marketing techniques using data acquired from customers. Exhibits include a sample checklist to review a Web site privacy policy, sample privacy notices for Web sites, sample privacy principles for posting on a Web site, and a sample Web site security checklist concludes the chapter.

Chapter 9: Insurance and Investment Services

The chapter describes the unique issues and concerns related to investment and insurance services and the collection of customer data. The medical privacy information privacy protection requirements are discussed in detail, as they related to insurance services and customer privacy. An investment and insurance information checklist is provided as an exhibit.

Chapter 10: Mergers, Acquisitions, Joint Ventures, and Affiliations

This chapter explores the issues of data privacy and data security when a merger, acquisition, new joint venture, or other type of relationship is created. Data privacy and data security per regulatory requirements are reviewed in detail, including the affiliation authority of the GLB Act, operating subsidiaries, protection of the privacy of nonpublic personal information, and information to be included in initial and annual notices of privacy policies and practices.

PART IV: REVIEW AND PERFORMANCE MEASUREMENT

Chapter 11: Monitoring Data Privacy and Controls for Data Sharing

If data sharing occurs, there must not only be controls in place to ensure proper compliance with regulatory requirements and internal policy, but also a monitoring system to ensure controls work. This chapter focuses on monitoring data privacy and data security. Sample control documentation and a sample set of internal audit procedures and checklists to review data privacy are provided.

Chapter 12: Examination by Independent Third Parties

Periodically, each financial institution is examined by its primary regulator to assess whether its internal policies, procedures, controls, and practices are in compliance with regulatory requirements. This chapter provides insights on those examination procedures, including detailed examiner questionnaires.

Chapter 13: Data Privacy and MIS Performance

To ensure data privacy and data security are properly controlled and protected, some form of management oversight reporting should be available. This chapter offers insights and examples of how senior management can monitor data privacy and data security.

Chapter 14: Identity Theft

This chapter covers the basic issues of identity theft and underscores the concerns regarding protecting customer privacy. The information provided highlights the significant increase in identity theft and the impact it is having on individuals as well as businesses and guides the reader on taking the first steps to address personal identity theft.

APPENDIXES

Appendix A: Glossary

Appendix B: Web Site Resources

Appendix C: FFIEC Training Resources (Available Only on CD)

Appendix D: Quick Reference Guide to Regulatory Issuances

Appendix E: Final Rulings on the Gramm-Leach-Bliley Act (GLB Act) (Available Only on CD)

THE VALUE OF THE CD COMPONENT

The public, political, and regulatory expectations regarding privacy have been emphasized frequently by regulatory issuances, directives, and settlement cases. The regulatory agencies will continue to be challenged to provide direction and definition regarding data privacy and data security in the financial services industry. Through issuances, bulletins, and other types of regulatory documentation, more information will undoubtedly be forthcoming.

The CD contains copies of the primary federal financial institution regulatory agencies' issuances regarding data security and data privacy. Navigate your way through the contents of the CD by reviewing the chart that contains the issuance title and description of how it relates to data privacy and protection. Each title is linked to a copy of the issuance and its attachments. You can also use the search engine to find exactly the content you are seeking. The User Guide in the manual describes the value of the CD and how to use it to your advantage.

