Letter from the Director

It used to be that banks spent more money on protecting the cash they held in their vaults than on anything else. The bars on the windows, security guards in the lobby, and armored cars were familiar signs of how important it was to protect the cash. These days, we know that another critical asset for a bank to protect is data.

Banks hold valuable data that, when compromised, allow criminals to steal an individual's identity and drain financial accounts. The potential for large financial gain has driven the demand by identity thieves for data. There are even secondary markets where thieves can purchase or trade data in mass quantities. There are people in the data theft industry whose "job" it is to obtain and aggregate as much data as they can. Others operate the elaborate black market operations where data can be bought and sold. And other participants are the actual end-users of the stolen information. Whether by manufacturing duplicate credit or debit cards, applying for credit in someone else's name, or using stolen online banking IDs and passwords to access someone's cash by originating transfers, the end-users are the criminals who actually convert the data into cash.

There are many reasons for banks to safeguard data. There are, of course, the regulatory requirements. In 2001, the Federal banking agencies implemented section 501(b) of the Gramm-Leach-Bliley Act by promulgating *Guidelines Establishing Standards for Safeguarding Customer Information.* The objectives of the guidelines and of the written information-security program they require are to (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. In addition, the guidelines require financial institutions to ensure that service providers with whom they contract implement a security program designed to meet the guidelines' objectives. Other laws, such as the Fair and Accurate Credit Transactions Act of 2003 and the USA PATRIOT Act, also require financial institutions to have in place strong policies and programs to safeguard customer data.

Another reason to protect customer data is to avoid financial losses to the bank. The costs associated with a data compromise can be great. They range from expensive insurance claims, to investigation and remediation costs, to the cost of providing free monitoring services for those affected. As important, however, banks need to safeguard data to protect against harm to their reputation and a loss of consumer confidence. If bank customers feel their bank cannot be trusted to protect their confidential information, they will go somewhere else. Although it has not yet happened to a financial institution, companies in other industries have gone out of business because of serious data breaches.

Everyone has a responsibility in safeguarding data. Financial institutions and their technology service providers have a legal duty to protect data, but consumers also have a responsibility to protect their own information. The FDIC has sponsored a number of symposiums around the country to educate consumers about the need to protect personal and confidential information from compromise. We advise consumers to always protect their Social Security number, credit card and debit card numbers, personal identification numbers, passwords, and other personal information. They should also protect their incoming and outgoing mail, properly discard any trash that contains personal or financial information, and keep a close watch on bank

account statements and credit card bills for any abnormalities.

The FDIC also has safeguards in place to protect our confidential data. As the steward of the deposit insurance fund and primary supervisor of more than 5,200 banks, the FDIC plays a vital role in maintaining confidence in the banking industry. In August, the FDIC issued updated procedures to examination staff as a reminder of the importance of safeguarding examination information—whether in paper, electronic, or other form. The updated procedures cover all documentation acquired or created in connection with a bank examination, such as reports of examination, examination work papers, bank information, and, especially, any sensitive bank customer information that may be gathered as part of a bank examination. The updated procedures (1) specify minimum standards for safeguarding examination information, including technical, physical, and administrative safeguards; (2) provide guidance for the implementation of an Information Security Incident Response Program with required procedures if an actual or suspected loss, theft, or unauthorized access of confidential or sensitive examination information is detected; and (3) incorporate recently issued guidance from the U. S. Office of Management and Budget requiring that security incidents involving personally identifiable information be reported within one hour after discovery.

The FDIC recognizes that even the best information security program may not prevent every incident. A critical feature of information security programs must be a plan for the bank to respond when incidents of unauthorized access to sensitive customer information maintained by the institution or its service providers occur. An incident response program provides a preplanned framework for dealing with the aftermath of a security breach or attack. In this issue of ***Supervisory Insights,*** "Incident Response Programs: Don't Get Caught Without One" highlights the importance of incident response programs and provides information on required content and best practices banks may consider when developing effective response programs.

We encourage our readers to continue to provide comments on articles, to ask follow-up questions, and to suggest topics for future issues. All comments, questions, and suggestions should be sent to SupervisoryJournal@fdic.gov.

Sandra L. Thompson
Director, Division of Supervision and Consumer Protection