Identity Theft: Is Your Security Blanket Tucked In?
November 07, 2005

Government regulations from Fair Credit Reporting to Gramm-Leach-Bliley offer financial institutions guidance to help keep personal information secure.

According to an oft-quoted 2003 Federal Trade Commission survey, nearly 10 million Americans --- or 4.6 percent of the adult population --- were victims of some form of identity theft, which cost consumers and businesses over $55 billion. Identity theft is the most frequent complaint to the FTC, with the number of complaints each year trending upward. According to the U.S. House Financial Services Committee, victims of identity theft on average spend 90 hours of their own time and $1,700 in out-of-pocket expenses in resolving the problem. Recently, several high-profile security breaches have focused public scrutiny on the vulnerabilities of companies' data security systems and the nexus between data security and the crime of identity theft. These incidents have renewed legislative and regulatory interest in this area, and almost every state in the country has introduced some form of identity theft notification bill.

For financial institutions that share personal financial information with business associates, protecting a customer's identity is vital. Unfortunately, no single federal or state law regulates the disclosure of nonpublic personal information. Instead, privacy and security regulations stem from a variety of specific state and federal regulations that restrict disclosure of consumer information in certain situations. Those same laws require that institutions that maintain personal information take reasonable steps to ensure the security and integrity of that information. At the federal level, these laws include, among others, the Fair Credit Reporting Act, the Fair and Accurate Credit Transaction Act (or the FACT Act), the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, the USA PATRIOT Act and the Health Insurance Portability and Accountability Act.

Disclosure of Personal Information

The Fair Credit Reporting Act is one of the oldest private-sector data protection laws. Although much of the Fair Credit Reporting Act focuses on maintaining the accuracy and efficiency of the credit reporting system, it also plays a major role in ensuring consumer privacy. This Act prohibits the distribution of "consumer reports" by consumer reporting agencies and credit bureaus, except for certain specified permissible purposes, and requires these entities to employ procedures to ensure that they provide consumer reports to recipients only for such purposes.

The FACT Act, passed in 2003, placed new obligations on financial institutions to prevent identity theft, entitled consumers to a free annual credit report from each of the three major credit bureaus and created a national fraud alert system to simplify a consumer's ability to detect and report fraudulent activity.

Provisions of the Federal Trade Commission Act prohibit unfair or deceptive acts or practices and give the Federal Trade Commission broad jurisdiction to prevent such

TEL 724.935.6789 CELL 412.760.6246 FAX 724.935.6790 DIRECT 724.935.2700
vdb@vmdlegal.com
4500 Brooktree Road, Suite 103 Wexford, Pennsylvania 15090
www.vmdlegal.com

practices by businesses. Prohibited practices include deceptive claims about the security and use of customer information.

Financial Institutions Give Notice

Of special interest to financial institutions is the Gramm-Leach-Bliley Act of 1999, which includes provisions to protect consumers' personal financial information and requires data security. The Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In return, consumers have the right to limit some sharing of information. Such limited sharing of personal financial information is highly regulated to help safeguard financial privacy.

Under the Act, "financial institutions" are defined as any entity that engages in financial activities, such as traditional banking, lending, insurance and related functions. For privacy purposes, commercial banks and thrifts, as well as any other entity that provides financial services, such as automobile dealerships and other retailers that finance their sales merchandise, are subject to the Act's privacy and security requirements.

Gramm-Leach-Bliley defines "nonpublic personal information" as any information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. This includes basic identifying information such as an individual's name, address, social security, account or telephone number.

To protect the security, integrity and confidentiality of customer information, the Act requires financial institutions to implement appropriate physical, technical and procedural safeguards. The federal banking agencies issued Interagency Guidelines Establishing Information Security Standards in March, 2001 to implement these safeguards. Specifically, every financial institution is required to implement a written information security program, approved by the institution's board of directors, which is designed to:

- ensure the security and confidentiality of customer information
- protect against any anticipated threats or hazards to the security or integrity of such information
- protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer
- ensure the proper disposal of customer information.

Amendments to the Security Guidelines, which address the risks associated with identity theft, became effective on July 1, 2005. The changes require financial institutions to develop, implement and maintain, as part of its existing security program, appropriate measures to properly dispose of consumer information.

The Security Guidelines require each financial institution to identify all reasonably foreseeable risks that could result in unauthorized disclosure or misuse of customer information, and assess the likelihood and potential damage that may result. Following this assessment, a financial institution must design a program commensurate with the sensitivity of the information and the complexity and scope of its business that

TEL 724.935.6789 CELL 412.760.6246 FAX 724.935.6790 DIRECT 724.935.2700
vdb@vmdlegal.com
4500 Brooktree Road, Suite 103 Wexford, Pennsylvania 15090
www.vmdlegal.com

addresses identified risks. The program should include:

- controls that authenticate and permit access only to authorized individuals, and that prevent employees from providing customer information to unauthorized individuals who may seek to obtain it through fraudulent means;
- background checks for employees with access to customer information;
- encryption of electronic customer information, including while in transit or in storage; and
- response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

The Security Guidelines direct every financial institution to require by contract that its service providers implement appropriate measures to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers. In addition, a service provider may be required to implement its own comprehensive information security program in accordance with the Federal Trade Commission's regulations.

Financial institutions must regularly monitor, evaluate and adjust their security program in light of changes in technology, sensitivity of the customer information and the institution's business and outsourcing arrangements. Training programs for the institution's employees are required. The institution also must provide its board of directors with annual reports regarding the status of the information security program and the institution's compliance with the Security Guidelines.

Effective Response – Federal and Customer Notification

Despite the safeguards, an institution's security program may fail. As noted above, Gramm-Leach-Bliley requires an effective response mechanism. In March 2005, the federal banking agencies issued guidance on the development of an effective response program designed to address incidents of unauthorized access to sensitive customer information. An institution's response program should contain procedures for:

- assessing an incident's nature and scope, and identifying what customer information systems and types of customer information have been accessed or misused
- notifying its primary federal regulator as soon as the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information
- file a timely Suspicious Activity Report in situations involving federal criminal violations requiring immediate attention
- taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information
- customer notification.

Under this guidance, the institution's primary federal regulator should be notified of all instances of unauthorized access to sensitive customer information, regardless of whether

TEL 724.935.6789 CELL 412.760.6246 FAX 724.935.6790 DIRECT 724.935.2700
vdb@vmdlegal.com
4500 Brooktree Road, Suite 103 Wexford, Pennsylvania 15090
www.vmdlegal.com

the customer is notified. "Sensitive customer information" generally means the customer's name, address or telephone number, in conjunction with the customer's social security, driver's license, account, credit or debit card number.

When an institution becomes aware of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine the likelihood that the information has been or will be misused. If the institution determines that misuse has occurred or is reasonably possible, it should notify the affected customer immediately. Notice may be delayed when a law enforcement agency determines that notification will impede a criminal investigation.

Conversely, customer notice is not required if the institution reasonably concludes that misuse of the information is unlikely and takes appropriate steps to safeguard the interests of affected customers. Finally, financial institutions are encouraged to notify the national consumer reporting agencies before sending notices to a large number of customers if such notices include contact information for the reporting agencies.

In adopting this guidance, the federal banking agencies sought to strike a balance between inundating consumers with notices that may be ignored and failing to notify them in situations where they may be harmed. This echoes the concerns raised earlier this year by Rep. Michael Oxley, Chairman of the House Financial Services Committee:

> "One of my concerns in this regard is that, given the dramatic rise in recent reports on data breaches, there will be a head-long rush toward notification in every instance. When no evidence surfaces to indicate that their information has been misused, consumers may begin to ignore these notices as just that many more pieces of unsolicited junk mail."

House Committee on Financial Services, Opening Statement of Hearing on Assessing Data Security: Preventing Breaches and Protecting Sensitive Information (May 4, 2005).

Currently, almost every state, as well as the U.S. Congress, has either enacted or is considering similar legislation. Although these bills vary somewhat, they incorporate the following common elements:

- **Entities Covered**: Any company that owns, acquires, licenses, collects or otherwise maintains personal customer information.
- **Personal Information**: Generally, consists of an individual's name plus at least one account, card or personal identification number.
- **Data**: Generally limited computerized or electronic data.
- **Definition of Breach**: Any unauthorized access and use of personal customer information.
- **Encryption**: Safe harbor for encrypted information.
- **Timing**: No prescribed time period for customer notification; generally, notification must occur as soon as practical.
- **Law Enforcement**: Notice may be delayed for law enforcement purposes.

TEL 724.935.6789 CELL 412.760.6246 FAX 724.935.6790 DIRECT 724.935.2700
vdb@vmdlegal.com
4500 Brooktree Road, Suite 103 Wexford, Pennsylvania 15090
www.vmdlegal.com

- **Form of Notice**: Generally, written notice is required, but e-mail, posting on a Web site or a press release is allowed in some instances.
- **Risk of Harm Exemption**: Reasonable likelihood of harm must occur.
- **Credit Bureau Notice**: Notice to credit reporting agencies may be required depending upon number of affected accounts.
- **Liability**: None of the bills address any liability issues and, currently, these issues are being addressed contractually and through common law principles.

Significant benefits are associated with the proper and legitimate use of customer information by a broad spectrum of governmental and private entities. These benefits should be considered in determining the appropriate legislative response to any information security breaches. Any state or federal legislation should not be too rigid or prescriptive in detailing the circumstances when customer notification is triggered, and should continue to include all governmental and business entities, and not just financial institutions, that maintain confidential or sensitive customer information.

TEL 724.935.6789 CELL 412.760.6246 FAX 724.935.6790 DIRECT 724.935.2700
vdb@vmdlegal.com
4500 Brooktree Road, Suite 103 Wexford, Pennsylvania 15090
www.vmdlegal.com