

# Secure Your Clients' Data

Failure to protect electronic information may yield business and legal risks

By **Jennifer Jackson Spencer**, founding shareholder, Spencer Crain pllc

**W**HEN IT COMES TO PERSONAL data regarding real estate, the Internet has created a transparent world. From local government Web sites that give property-tax information to sites that compare home-sale prices and values, records that previously only could be secured in person at a local government office are now available online.

There's a vast difference, however, in the transparency of this information and the requirement to protect individuals' personal identification and financial data. Consumers are extremely sensitive to any threat involving their personal or financial information. As such, mortgage professionals and the financial institutions with which they work must inspire absolute trust. Being seen as cavalier or incompetent at protecting consumer privacy would be a major blow in the marketplace — and a major legal problem.

## Statutes for electronic data storage

Personal data stored on computers are subject to a wide spectrum of security risks, ranging from illegal activities — such as hacking and data piracy — to careless ones, such as losing a laptop computer that contains sensitive information.

Since the late 1990s, federal statutes such as the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Fair Credit Reporting Act, the Electronic Communications Privacy Act, and the Fair and Accurate Credit Transactions Act, in addition to state statutes, have created a substantial body of regulations governing the collection, use and security of personal financial and medical records. They also impose penalties on companies that do not comply with their provisions.



Two interrelated statutes are of particular importance to mortgage professionals. The Gramm-Leach-Bliley Act requires all financial institutions to adopt a privacy policy and to give consumers written notice of the policy's terms, with the opportunity to opt out. The Electronic Signatures in Global and National Commerce (ESIGN) Act allows banks to store records of loans, accounts and other transactions in electronic format. ESIGN requires electronic-storage systems to maintain these records' accuracy, integrity and accessibility.

Financial businesses implementing an electronic storage system should seek the advice of legal and auditing counsel about structuring their system for litigation discovery, audit support and bank-examiner access. There should be adequate controls on access and personal-data privacy to maintain record-integrity and to

comply with the Bank Secrecy Act, the Gramm-Leach-Bliley Act and similar statutes.

Other ways to determine whether a bank or lender has an acceptable electronic storage system are if it:

- **Is consistent with the bank's general records management and retention policy;**
- **Has adequate security to prevent cyber-crime and other unauthorized access;**
- **Provides for extensive backup and recovery (a special focus for bank examiners); and**
- **Makes electronic records fully available for discovery during litigation,** in accordance with the revised Federal Rules of Civil Procedure.

## Practical steps

When it comes to protecting data privacy, mortgage professionals who have their own offices also should focus on any information that is secured or transmitted over the Internet, particularly through Web site information and "contact us" pages.

If your company collects or receives personal data from customers or prospects via the Web, these elements should be part of your privacy protection standards:

- **Notice of information practices:** If a company collects nonpersonally identifiable information on its Web site, there should be a clear and conspicuous notice on the site about the collection policy. If personally identifiable information is collected, the notice should appear before such information is collected. These notices also should disclose any consequences of an individual's refusal to provide information.
- **Choice on how personal information is used:** Once consumers are informed about a Web site's information collection policies, they should be clearly informed about any changes in these policies. These changes should not be applied to previously collected information. Consumers also should have the opportunity to opt out of the new policies. Previously collected



**Jennifer Jackson Spencer**, founding shareholder of Spencer Crain pllc in Dallas, is an experienced trial lawyer highly regarded for her knowledge of e-discovery issues. She counsels clients, from *Fortune* 500 corporations to midsized public and privately held companies, in a broad spectrum of industries. The firm is majority-owned by women and certified by the Women's Business Enterprise National Council. Contact Spencer at [JSpencer@spencercrain.com](mailto:JSpencer@spencercrain.com), (214) 290-0000 or via [www.spencercrain.com](http://www.spencercrain.com).

Continued ...

REPRINTED FROM *SCOTSMAN GUIDE* RESIDENTIAL EDITION AND [SCOTSMANGUIDE.COM](http://SCOTSMANGUIDE.COM), DECEMBER 2008

All rights reserved. Third-party reproduction for redistribution is prohibited without contractual consent from Scotsman Publishing Inc.

## Secure Your Clients' Data

... Continued

nonpersonally identifiable information should not be linked to personally identifiable information without explicit consumer notice and opt-out opportunity. There also should be a clear and conspicuous notice of the opt-out choice for nonpersonally identifiable information collected for profiling, generally by advertisers. Sites with multiple advertisers should have a single opt-out screen.

■ **Access to collected information:** Consumers should have reasonable access to personally identifiable information and other information any Web site advertiser retains for profiling.

■ **Security for collected information:** There should be reasonable policies to ensure that any collected personal information is protected from misuse, alteration, destruction or improper access.

### Legal risks

There has been a rising tide of lawsuits filed on behalf of consumers and employees who claim their personal data may have been compromised. Highly publicized reports of personal-records theft involving financial institutions,

**“Consumers are extremely sensitive to any threat involving their personal or financial information. As such, mortgage professionals and the financial institutions with which they work must inspire absolute trust.”**

e-commerce businesses and government agencies pose increased litigation risk over actual or potential identity theft based on allegations that companies have not fulfilled their data-security obligations.

Targets have included software companies, security-system vendors, records-management services, management consultants, employment agencies and even cleaning-service contractors. Banks, credit unions, credit card companies and other businesses may sue suppliers to recover the costs they incur from a security problem. This area of the law, where few precedents exist, likely will become more active.

Facing the possibility of litigation, many

companies are pressuring their information-technology (I.T.) vendors and contractors to enforce stronger data-protection steps. I.T. contractors must be prepared to document the security of their internal processes and their employees. Sophisticated customers may require adherence to the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) 70, which defines data-security safeguards. In addition, I.T. service contracts increasingly specify customer-notification procedures in the event of a security breach, such as the loss or theft of a laptop computer containing sensitive data.

■ ■ ■

The use of electronic and online technology to collect, process, archive and exchange sensitive personal information has increased the speed and efficiency of real estate and mortgage professionals. Simultaneously, however, it has increased the legal risks for compiling and using the data.

If you are unsure how secure the personal data you collect and store is, the time to get information-security and legal guidance is now — not after a hacker strikes or a laptop goes missing. **!**