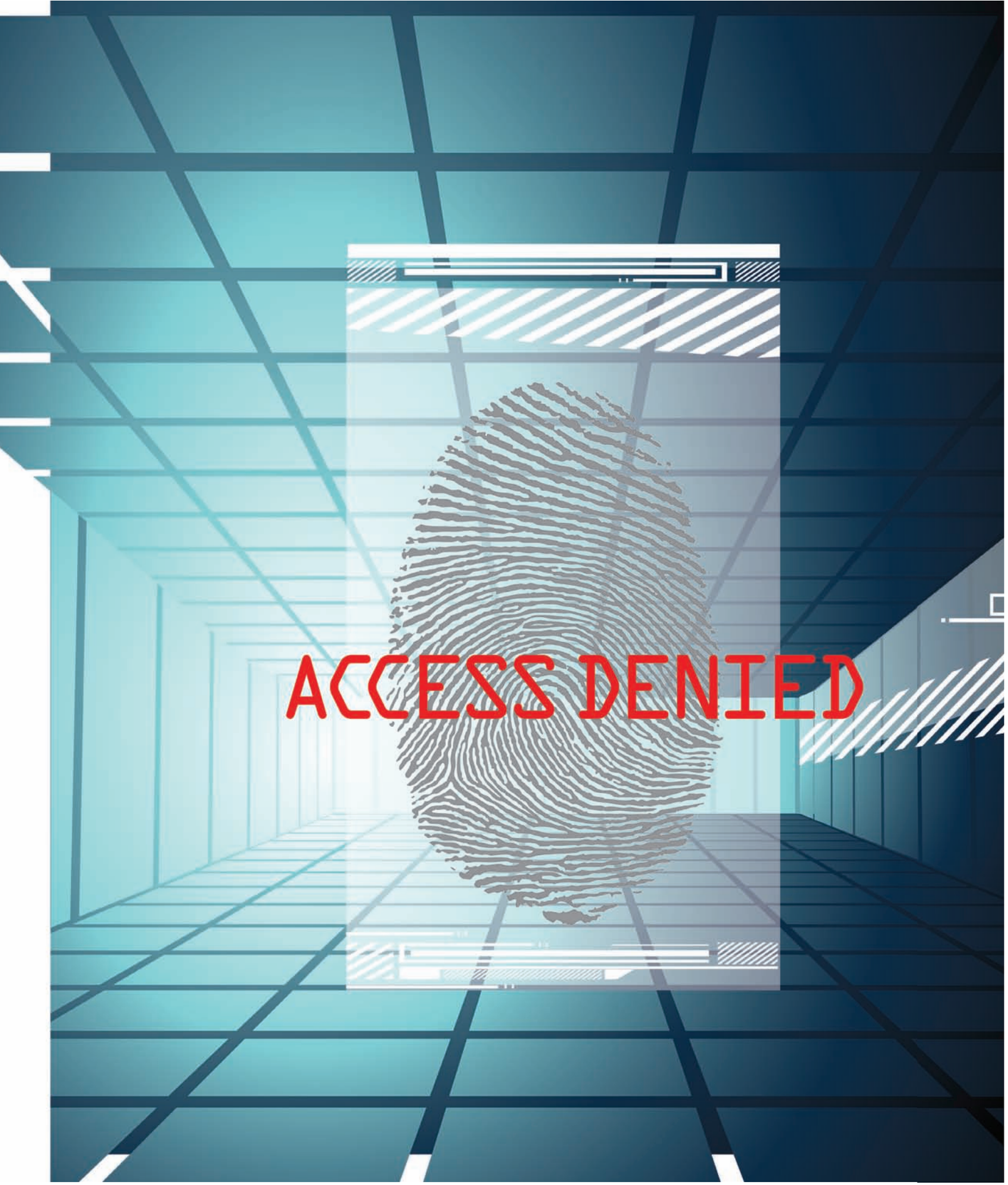


DATA SECURITY ADVANCES

Especially in the current market, lenders need to consider if they are keeping ahead of the thieves.

by Scott Kersnar

Uncertainty about the economy and their own prospects has made a lot of people very jumpy about the security of their financial data. At the same time, consumers are still eager to Twitter one another and share all kinds of MySpace and FaceBook information and to have hand-free cell phone access via Bluetooth. Unfortunately for Bluetooth users, would-be hackers need only go to Google to see how many Bluetooth sniffers, Bluetooth address spoofers and Bluetooth hacking tools are readily available.

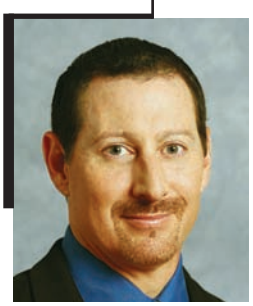
President Obama's high-profile announcements about assessing security threats to electronic communication has made some mortgage lenders think harder about their own vulnerabilities. "There are no Bluetooths at LSSI," said Cary Burch, CEO of San Diego-based Lender Support Systems Inc., a provider of lending and loan-servicing software.

Has the mortgage industry as a whole made recent gains in consumer and regulatory confidence regarding data security issues? "I think not," he said. "I think our industry is asleep at the wheel."

Mr. Burch is not alone in his concern that the mortgage industry has lagged in addressing data security. Back in January 2008 Minneapolis-based Wolters Kluwer Financial Services released a survey warning that "only one-third of financial institutions using the Internet to send confidential documents to customers, partners and service providers are doing so using a secure electronic document delivery solution," according to a recent WKFS survey. While nearly 62% of the 347 responding banks, credit unions and mortgage companies said they transmit confidential documents such as loan disclosures and documents via the Internet, only one-third say they are using a secure electronic delivery solution.

"A secure, electronic delivery system that encrypts sensitive data so only the sender and receiver can view can help better protect confidential data and documents," commented WKFS vice president and general manager Jason Marx. "The return on investment of implementing such a system can be well worth it for a financial institution when they consider the financial, legal and reputational risk tied to a data breach."

Bluetooth hacker and missing laptop news stories don't banish criminality and carelessness. Human misconduct rather than software flaws account for many security breaches. Like companies in other industries, said Mr. Burch, most mortgage lenders fail to take proper measures to prevent insider data theft. He cited a Ponemon Institute survey of 945 adults in which 59% of surveyed employees said they would take something of value with them when they leave the company. All those surveyed "had access to proprietary information such as customer data, contact lists, employee records, financial reports, confidential business documents, software tools or other intellectual property." Meanwhile, "only 15% of respondents' companies reviewed or audited the paper documents or electronic files employees were walking out of work with."



Human misconduct rather than software flaws account for many breaches. Like companies in other industries, most mortgage lenders fail to take proper measures.

—Cary Burch LSSI

As malicious attacks by disgruntled former employees are expected to rise, spending on security is predicted to fall. A recent *Information Security* magazine survey showed that while data protection, threat management and other security initiatives are top concerns for financial institutions, 27% of those surveyed said they expect their security budgets to remain flat, 23% are delaying some security purchases and over 50% expect security budgets to shrink if the economy doesn't rebound.

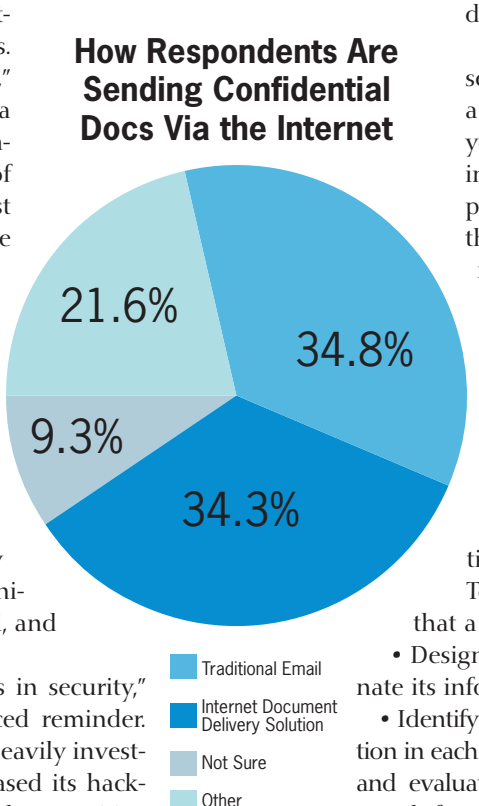
Citing that survey, Mike Nell, vice president of information technology, iStream Financial Services, Brookfield, Wis., said the cost of security services has to be measured against the gravity of the threat rather than the disappointing state of many companies' revenue. "No single event could so quickly take a company down as to have your confidential information hacked and exposed," he warned. He said consulting companies like iStream "provide an external set of eyes" to monitor threats.

Intrusions via "social engineering" pose a threat commonly overlooked, warns Randy Schmidt, president and founder of mortgage-industry service provider Data-Vision, Mishawaka, Ind. "Social engineering is typically an intruder's clever manipulation of people's inherent tendency to trust others," he said. "The intruder's goal is to obtain information that will allow them to gain unauthorized access to valuable information or systems within the organization. The weakest link in security system and processes is typically people's willingness to accept someone at their word." As an example, he said, "you might get a message supposedly from the HR department saying: 'We are implementing a new version of PeopleSoft', or some other popular product, and be asked to visit a website and sign in. The site can then capture the login information and attempt to use your login credentials to breach your network security."

What actually can be done quickly to promote industrywide data security? Publishing a security policy and appointing an employee to oversee implementation is not enough, said Gabe Minton, chief strategy officer for Greenwood Village, Colo.-based Motivity Solutions and former vice president of industry technology for the Mortgage Bankers Association. "Lend-

ers and service providers alike need to recognize that this is a situation that needs to be dealt with from the top level of an organization down."

While he offered no studies to confirm his view, Mr. Minton said he believes the mortgage industry has made some strides in protecting data in motion over the months since the WKFS survey was done, by greater use of virtual private networks, encryption and other measures. "A more important threat is data at rest," he said, "data stored on a laptop or in a data in a SQL database that is not encrypted. Hackers want to grab a lot of data at one swipe. Securing data at rest starts at the organizational level." He said there has been progress there as well, particularly by banks and other regulated financial institutions. "If you go into banks these days, you see that the banks are pretty locked down. They disable the USB ports on their computers to prevent employee data theft with thumb drives. They also disable websites to prevent data downloads." He said data-quality dashboards are now available to monitor "how often a data field has changed, and who has touched it."



Source: Wolters Kluwer Financial Services.

However, "there are no silver bullets in security," commented Mr. Nell in a widely voiced reminder. While we hear that organized crime is heavily invested in cybercrime and China has increased its hacking efforts into U.S. government and other sensitive databases, there also are no uniform national laws governing data security breaches. On all sides we are reminded that the legal safeguards against data thieves and hackers comprise a patchwork of state and federal laws aimed at specific sectors. While the health-care industry is governed by HIPAA, FCRA and FACTA apply to consumer-credit transactions and Gramm-Leach-Bliley covers financial services.

Some observers point to the Federal Trade Commission's Safeguards Rule as the closest thing we have to a national data security standard. In January of this year the FTC filed a complaint against an individual Nevada mortgage broker who compromised borrower privacy and financial data by tossing old files in a Dumpster. In November 2008 the Federal Trade Commission announced settlement of a complaint against Texas-based Premier Capital Lending for violating the FTC's Safeguards and Privacy Rules and Section 5 of the FTC Act. Premier was charged with negligently allowing a third party to access borrower data. Consequently a hacker obtained the lender's credentials and using them to access hundreds of consumer reports.

If you go to www.ftc.gov, and do a search for "safeguards rule," you will see a detailed explanation of the measures your company should be taking to be in compliance. Under the rule-making power granted to the FTC by Congress, the Safeguards Rule applies to all financial institutions, including "check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers and courier services." They/you also are responsible "for taking steps to ensure that their affiliates and service providers safeguard customer information in their care."

To be in compliance, the FTC requires that a company:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards program, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Alain Sheer, a staff attorney in the FTC Division of Privacy and Identity Protection, said that the Safeguards Rule mandates "reasonable security" rather than rules for rules' sake. The overarching rule for sequestering sensitive consumer information is not to collect it in the first place if you don't need it, to

keep it only as long as necessary if you do collect it, and to dispose of it properly when you no longer need to use it. "The Dumpster is still the goldmine for identity theft," he reminded. He stressed the need to develop a written retention policy to make sure you keep only the information you need for business reasons or compliance. He urged checking the default settings on computers to make sure you aren't unnecessarily keeping credit card numbers, etc. Mr. Sheer stressed the importance of making sure employee training in security issues is thorough and that employee compliance is carefully monitored. He warned that monitoring contractor security has to be rigorous.

The FTC details requirements governing employee data handling, detecting security failures, disposal of consumer information and other critical requirements. To remain in compliance, companies should "consider notifying consumers, law enforcement, and/or businesses in the event of a security breach," said the FTC guide. Thus, when LendingTree discovered that several of its employees had created a security breach by giving five Southern California lenders password access to customer information contained in LendingTree's loan request forms, LendingTree sent out a letter so informing its customers, even though LendingTree said it did not believe any identity theft or fraudulent financial activity resulted from the breach. LendingTree's security policy is available at www.lendingtree.com/legal/security-policy.

LendingTree's digital certificate and public key infrastructure provider is Jersey City, N.J.-based Comodo, a 2007 Hot Companies award winner that bills itself as "the second-largest issuer of high-assurance digital certificates in the market." Comodo also offers code signing, content verification and e-mail certificates; PC security software; vulnerability scanning services; secure e-mail and fax services. "LendingTree's need for digital certificates is rather large," said Len Gangi, Comodo vice president of enterprise solutions, "and managing digital certificates across all their websites and network operations requires an administrative tool we call Comodo Certificate Manager." He said the tool also helps LendingTree address compliance.

Lenders and service providers alike need to recognize that this is a situation that needs to be dealt with from the top level of an organization down.

—Gabe Minton
Motivity Solutions

Mr. Minton said industrywide technology standards can offer data-security safeguards. "I think everyone is committed to using MISMO standards," he said, pointing to the MISMO Version 3 SMART Docs with tamper seal as the arrival of a solution that is "what MISMO should have been developing all along." Motivity Solutions' Movation lending optimization software platform is built on MISMO standards. By combining a company's existing systems, it promotes consistency in data handling and serves as a risk-protection platform.

Like advanced systems used in other industries, Movation employs the least privileged security model, which gives users only the privileges absolutely necessary to perform any given task. "Movation has greatly improved data security and quality within our lending operation," said Calvin Hamler, CEO of Assurity Financial Services LLC, "first by encrypting data in motion as it moves into and out of our systems, and second, by encrypting data at rest at the database level whenever it is not in use by one of our systems. Further, the least privileged security model creates user and role based access mechanisms to assure that no one will access data unless given permission. Movation takes this a step further by automating validation checks on data throughout the origination lifecycle."

He went so far as to say that Movation "addresses an important need in the industry that we believe will help stimulate lending again. Our investors will have new degrees of confidence in the data they are making execution decisions on because we will not only be able to score the data for a loan with the technology, but will have robust logging of exactly what changed when and by whom. Investors will be more confident in their decisions, and will experience fewer problem loans."

Englewood, Colo.-based Assurity shows its concern for restoring consumer confidence in the mortgage industry by posting an auditor's letter of commendation on its website. The letter from auditor Richey, May & Co. says Assurity conducts its business operations "at the highest level of integrity and honesty." Companies like Motivity help like-minded lenders do the same. MT

Start a new thread TODAY.

Mortgage Grapevine

- Interact with industry experts
- Ask questions of your peers
- Exchange ideas & scenarios

A GROWING AUDIENCE OF OVER **60,000** ACTION-ORIENTED MORTGAGE PROFESSIONALS HAVE ALREADY JOINED THE **MORTGAGE GRAPEVINE** COMMUNITY.

Mortgage Grapevine - brought to you by Broker Universe is a unique resource for mortgage professionals to share unique borrower scenarios and ask advice from fellow colleagues.

Visit the Mortgage Grapevine at **mortgagegrapevine.com** and interact with your colleagues & potential business partners.

- Exchange ideas
- Discuss current issues
- Get advice for your tough loans

For more information on advertising on Mortgage Grapevine or any of our online products , please contact Justin Nathan, Online Advertising Sales Manager, at (212) 803-8671 or Justin.Nathan@Sourcemedia.com

BrokerUniverse

SourceMedia