

THE BUFFALO NEWS  
**BUSINESS TODAY**

November 9, 2008

## **New protections going into effect against I. D. theft**

### **Law obligates financial institutions now, other sectors of U. S. business next year**

By Jonathan D. Epstein NEWS BUSINESS REPORTER

Corporate America is taking on a new responsibility: protecting your identity.

As of Nov. 1, banks — and soon a wide range of other companies — are required to take extra steps to ensure they can detect and prevent fraud related to identity theft. They also have to develop better procedures to notify victims.

If they don't, they could face fines, regulatory penalties, lawsuits and public embarrassment — not to mention a loss of reputation and business.

“As a financial institution, we're dependent on the customers' trust,” said Frank Polino, executive vice president of operations at First Niagara Financial Group. “We need to make sure we're doing all the necessary steps to make sure their confidential data is safeguarded.”

The new initiative marks an effort to respond to a growing perception among Americans that businesses and even government entities are keeping too much personal information and not securing it. That's a result of an endless series of computer break-ins and mishaps that have exposed millions of consumers to fraud.

Government and industry leaders are worried that such incidents and resulting fear will cause consumers to lose confidence in business. As a result, people may cut back their shopping and purchases altogether, or at least stop using the Internet and other technology that American businesses have spent billions of dollars investing in. And that would severely damage a struggling economy.

“People will start thinking banks and companies are not secure or will stop shopping online or stop going to certain places,” said Tom Harkins, chief strategy officer at technology firm Secure Identity Systems in Tennessee. “The whole consumer confidence starts to waver and it has a trickle-down.”

To prevent that, the government is mandating that businesses do a better job of protecting customers. Under the new regulations, banks and other companies must look at how they open accounts for products or services, and how they verify a new customer's identity.

They must assess all possible scenarios that could put a consumer at risk of being a victim of identity theft and fraud. And they have to develop “reasonable policies and procedures” to respond to each possibility of risk, whether it's suspicious behavior, dormant accounts, forged documents, inadequate identification, changes of address or other “red flags.”

They also have to train staff, keep their program updated and report annually on its effectiveness. And they must have a plan for notifying victims.

“It's in our interest and our customers' best interests to do what we can to mitigate identity theft,” said John Krenitsky, enterprise compliance officer for M&T Bank Corp.

Known as the “red flag rules” and announced a year ago, the new regulations were authorized by the Fair and Accurate Credit Transactions (FACT) Act, which Congress passed in 2003. The rules were enacted not only by the banking agencies — the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve Board and the Federal Deposit Insurance Corp. — but also the Federal Trade Commission.

That ensures that not only do they apply to banks and credit unions, but also mortgage lenders, credit card issuers, small business lenders, debt collectors, insurers, retailers, car dealers, utility companies, phone companies, municipalities, landlords or property managers, health care companies, elective surgeons, jewelers, and any other company that looks at consumer credit and holds consumers' personal information. More than 2 million firms are affected.

“Unless we start doing something quickly, there will be so many consumers hurt that the whole economy could suffer,” Harkins said. “We have to do a much better job.”

## THE BUFFALO NEWS

# BUSINESS TODAY

So instead of relying on a document someone presents or taking someone's word, companies must now use a database or service that can track and verify the information.

"Years ago, they just took a driver's license, but most of us realize it's pretty easy to counterfeit a driver's license," Harkins said.

The FTC recently delayed enforcement of its rule until June 1 to give the industries it oversees more time, because many non-financial companies are unaccustomed to such requirements, were still unaware of them, or were not yet ready. The rule was still effective Nov. 1, however, and bank agencies are enforcing it now.

"The speed limit is in effect, but you can breathe because they're telling you that the radar guns aren't on until May 1," Krenitsky said.

This isn't the first time industry and regulators have tackled the problem. Banks have already sought to monitor transactions for suspicious or unusual behavior. And both industry and government have focused on helping consumers prevent, discover, and respond to theft.

Regulators are also encouraging companies to maintain an effort to stop "phishing." That refers to the use by criminals of spoof e-mail messages and Web sites that resemble legitimate companies or entities in an effort to get consumers to give up their account numbers, sign-in names, and passwords.

So companies should now have a system in place, using internal resources or outside services, to monitor the Web for fake e-mails and sites, and take them down immediately. That can be difficult because many of these sites are hosted in foreign countries where the laws are different than in the United States.

"We've gotten much better at being able to close down the fraudulent Web site very quickly, and the vast majority of those emails never make it to a recipient," said Matt Speare, senior vice president for technology infrastructure at M&T Bank Corp.

Banks also tightened their Internet security, first voluntarily and then at the insistence of regulators. Besides "firewalls," banks also implemented software to cut off malicious attempts to hack into its site and prevent fraudulent access.

"We are constantly assessing the changes in threats," Speare said. "We have been fortunate to stay ahead of the threats."

Most significantly, where a simple password was sufficient for a customer to access their bank account online in the past, banks are now required to use stronger means to verify someone's identity first. That requirement, imposed by the government as of yearend 2006 and often referred to as "multifactor authentication," means customers have to pass at least one more "challenge" before gaining entry.

Banks track customers' usage and habits, so that they can tell where, when, and how a customer normally logs in. If a customer seeks to log in as normal, such as from their home computer using the same software as always, the minimum challenge would be used, perhaps even just the regular password.

But if the attempt comes from someplace unusual — say, an Internet cafe in Eastern Europe — or otherwise breaks the pattern, it could be viewed as suspicious and more challenges would be required.

"If you normally sign on from Buffalo and an hour later, you sign on from Singapore, that might trigger an alert or question," said David Miner, senior director of financial services industry solutions at software firm Syman-tec Corp.

The challenge could involve one or more rotating questions previously selected and answered by the customer or the use of an image with a corresponding phrase that the customer has to type in. In either case, the customer sets up the challenge when they first register with the bank. And they must provide the answer to gain access.

"If you continuously dial in from Clarence, you may never know it exists," said Michelle Trolli, M&T executive vice president and chief information officer. "But if all of a sudden, you're dialing in from the Ivory Coast, you'll

THE BUFFALO NEWS  
**BUSINESS TODAY**

be challenged.”

On the Web, banks also may have to prove they're for real by displaying a preselected image the customer has chosen. The combination provides reassurance to both the customer and the bank that the other is legitimate.

Some banks also provide commercial customers with single-use “tokens,” which are devices linked to the bank's central computer system. The tokens generate constantly changing codes that must be typed in within an allowed time frame.

“The threat continues to evolve, and the bad guys learn how these systems work and figure out ways around them,” Speare said. “It's a constantly evolving process. We relook at this issue every six months.”

#### **ABOUT SECURE IDENTITY SYSTEMS**

Secure Identity Systems is the leading provider of fully managed, total identity theft protection systems that safeguard financial institutions, businesses, individuals, and households. For more information, visit <http://SecureIdentitySystems.com/>.