

How to Measure a Well-Run Automotive Finance ...

'Red Flag' Rules For Banks Target Identity Theft

June 2, 2008 8:16:00 PM PDT

By: [Greg Bordonaro](#)
Hartford Business Journal Staff Writer

Banks have until November to implement new federal "red flag rules" aimed at curbing [identity theft](#) by protecting the most sensitive data they keep on their customers, including deposit account and personal information.

The vulnerability of that data was exposed last month when a backup tape containing vital information on more than 550,000 Connecticut depositors and investors was lost while being transported by a storage company working for the Bank of New York Mellon.

As Connecticut residents receive their notifications of the security breach, local banks are working behind the scenes to establish the procedures required under the new law.

Connecticut banking officials noted that the [red flag rules](#) aren't aimed at preventing the incidents like the missing computer tape. Rather, they are meant to prevent fraud after the sensitive information it contains falls into the wrong hands.

"You can only legislate so much to prevent things like this from happening," said Barry Abramowitz, senior vice president and chief information officer of Liberty Bank in Middletown. "They knew what they were supposed to do, but they didn't do it. It's universally acknowledged that you don't send out any unencrypted data with customer information."

16 Thefts Per Minute

A survey conducted by the [Federal Trade Commission](#) in 2006 found that 8.3 million Americans, or 3.7 percent of the adult population, were victims of some form of identity theft in 2005. That means about 16 U.S. adults had their identity stolen every minute that year.

Now that sensitive information, including names, birth dates, Social Security numbers and bank account details for hundreds of thousands of Connecticut residents is lost — and possibly in the hands of potential identity thieves — Connecticut banks are taking steps to minimize the damage.

"The banking industry has always been subject to very strict regulations when it comes to preventing and detecting identity theft," said Lindsey Pinkham Senior Vice President and Secretary of the Connecticut Bankers Association. "This regulation codifies existing precautions taken by financial institutions."

The purpose of the new regulation, which will apply to all financial institutions and businesses that provide credit or allow payments or transactions by consumers and small businesses, is to authenticate the identities of customers, essentially to ensure that people are who they say they are, Pinkham said.

It will force financial institutions to implement a [written theft prevention program](#) to detect and prevent identity theft in connection with new or existing accounts.

The written program must be able to identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft, and then respond to them appropriately.

Change Of Address

Jorge Santiago, vice president and branch administrator of Milford Bank, said his bank already has been very aggressive in detecting identity theft associated with a change of address. He said his bank does not accept address changes over the phone. Instead, it requires a written note signed by the customer so they can compare the signature to a previously signed check.

He said the red flag rules have been relatively easy to implement.

"I would hope for most banks this is just formalizing many of the procedures they are already performing to protect customers from possible identity theft and fraud," Santiago said.

Other local bankers see it differently.

"It's a little overkill," said Bill McGurk, president and CEO of Rockville Bank. "The regulation is redundant, forcing us to institute rules and procedures we already have in place. It's also an unfunded mandate. If you are already doing it right in the first place, then why should you go through the process again."

Karen Bryant, vice president and compliance/security officer of Rockville Bank, said redundancy exists because the regulation requires banks to show a separate risk assessment of all its processes, products and services based on the [red flag indicators](#). They must then cross reference the red flag rules to their current procedures.

Bryant tends to agree with consumer groups that have argued that the rules give banks too much discretion over how to implement their [written program](#).

"There may be a danger in flexibility only because everyone can interpret the rule differently," Bryant said.

'Tailoring' The Rules

Susan Stawick, a spokesperson for the [Federal Reserve](#), said that the flexibility was necessary so written programs "can be tailored to the institution's size, complexity, and the nature of its operations."

Auditors will be checking to ensure proper [red tag guidelines](#) and precautions are instituted at financial institutions, said Pinkham, noting that [penalties](#) may be imposed on those who fail to comply.

Change of address followed by unusual customer activity such as a request for an additional or replacement debit card, is one of the most common indicators of identity theft and fraud that the program is supposed to detect.

Other common indicators the program should detect include unusual credit activity such as an increased number of accounts or [inquiries](#), documents provided for identification that appear altered or forged, phone numbers associated with pagers or answering services, a lack of correlation between Social Security number range and date of birth, and personal identifying information associated with known fraud activity.

[Back to blog homepage](#)

[Read more...](#)