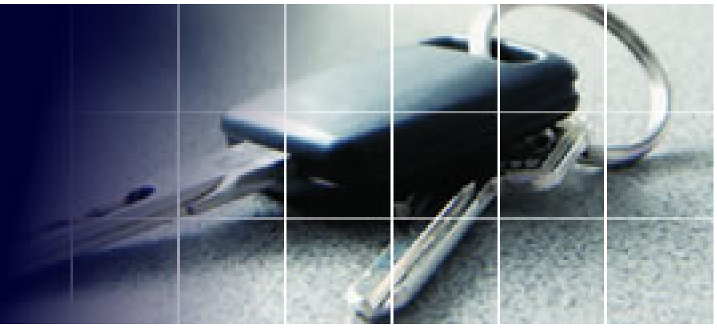
Crowe Horwath™

Dealership Flash



July 2008

Dealership Flash offers up-to-date information on issues affecting retail dealers. Each month, this electronic communication from Crowe Chizek and Company LLC features pertinent articles written by retail dealer specialists who have in-depth, practical knowledge about dealerships. To receive *Dealership Flash* via e-mail, please visit www.crowechizek.com/dealer.

Identifying Identity Theft: Complying With the New Red Flag Regulation

By Kelly L. Faehr, CPA

Identity theft has cost Americans an estimated $15.6 billion in losses in recent years. To help combat this growing epidemic, a new red flag regulation has been passed to protect consumers. Author Kelly Faehr details what is required of dealers to comply with the new regulation and how the requirements affect the dealership industry.

Along with financial institutions and other creditors regulated by the U.S. Federal Trade Commission (FTC), dealerships face a new regulation to prevent and detect identity theft. To avoid potentially hefty fines and penalties, dealers need to take note of the Identity Theft Red Flags and Address Discrepancies regulation that takes effect on Nov. 1, 2008, and modify their systems and practices accordingly.

Regulatory Requirements
In November 2007, the FTC and federal financial institution regulators issued final rules and guidelines for implementing Sections 114 and 315 of the *Fair and Accurate Credit Transaction Act of 2003* (FACT Act), which includes the red flag regulation.[1] Section 114 requires financial institutions, defined to include motor vehicle dealers, and other creditors to develop and implement a written identity theft prevention program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts, often referred to as "covered accounts." Dealers must also institute a program to review their identity theft program regularly to update or modify it as needed. Section 315 of the FACT Act provides guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

Under the new regulation, dealers must implement an identity theft program that identifies, detects, and reacts to red flags raised to indicate identity theft. The new rules will require dealerships to automate as much of their compliance activity as possible and will require constant training of sales and finance and insurance personnel.

Previous regulations, such as the *Gramm-Leach-Bliley Act of 1999* and other information security guidance, sought to safeguard information. The new regulation tackles identity theft from a different angle: It assumes that a criminal has already obtained consumer information and is now attempting to use that information.

Dealerships are bound by the new regulation because they are considered creditors based on the products and services they provide. Also, since covered accounts include accounts created to permit multiple payments or transactions, sales of vehicles financed through a retail installment sales contract are covered by the regulation.

Instituting an Identity Theft Prevention Program
Some of the safeguards required to comply with the new regulation might already be in place at some dealerships. For example, your employees may already verify an applicant's address against consumer reports. For many, however, the task could be cumbersome and costly: Systems will need to be implemented to train employees so they are able to recognize pertinent red

Under U.S. Treasury rules issued in 2005, we must inform you that any advice in this communication to you was not intended or written to be used, and cannot be used, to avoid any government penalties that may be imposed on a taxpayer.

flags and take appropriate action; automate as many compliance functions as possible; generate annual reports; and review at least annually the effectiveness of the current system and identify areas that need to be updated or modified.

A dealership's identity theft prevention program must be appropriate to the size and complexity of the dealership. The larger your business and the more employees who work with credit applicants, the more detailed your program will need to be. Program policies should ensure that the dealership is prepared to:

- Review red flags and identity-theft-prevention practices already incorporated into the dealership's program;
- Identify relevant red flags that might arise in the course of a transaction with a buyer;
- Respond appropriately to any red flags that are detected; and
- Periodically update the program (including which red flags are considered relevant) to reflect changes in risks to customers and to the safety and soundness of the dealership from identity theft.

A dealership must also designate a person to serve as its program's manager. This person will be charged with monitoring on a regular basis the effectiveness of the dealership's program, new trends in identity theft, and any updates in the regulation and will need to modify the dealership's program accordingly. The program manager must also generate annual reports on the program's effectiveness.

Red Flag Requirements

A red flag – a pattern, practice, or specific activity that indicates the possibility of identity theft – falls into one of five categories:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information;
- Unusual use of or suspicious activity related to a covered account; and
- Notices from customers, victims of identity theft, law enforcement authorities, or others regarding possible identity theft in connection with covered accounts.

The red flag regulation includes guidelines that offer a list of 26 types of red flags and instructs organizations to review activity for signs of these flags. These guidelines include how to identify relevant red flags, typical scenarios in which identity theft is more likely to occur, how to detect the existence of red flags, steps to take to prevent or mitigate identity theft when a red flag is detected, and how to update the program to keep it current. Some examples of red flags as noted by the FTC include:

- Verifying that the date of birth and Social Security numbers provided by a customer match the accepted ranges;
- Verifying that the address provided by a consumer during a credit transaction matches the consumer's address provided to the dealer by consumer credit reporting agencies;
- Determining whether a customer's address, Social Security number, or phone number is the same as that submitted by other credit applicants; and
- Determining that personal information submitted by a customer is not consistent with information already on file for that person.

Once a red flag has been detected, the dealership is required to take action. The regulation lists nine possible actions that could be appropriate when a flag or flags are triggered:

Under U.S. Treasury rules issued in 2005, we must inform you that any advice in this communication to you was not intended or written to be used, and cannot be used, to avoid any government penalties that may be imposed on a taxpayer.

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to the covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

Processes should be in place for taking each of these actions, including how to determine which action is appropriate; how to notify dealership management of the red flag and action being taken; what steps must be taken to follow through on a particular action; and how to document the entire process so the program manager can include the incident in the reporting.

Balancing the Challenge

Owing to the number of flags and the volume of potential transactions in which these flags might be found, the challenge for most dealers can seem daunting. Particularly challenging will be managing consumer expectations of quick responses when processing transactions against complying with the regulations and the processes you've developed. In the long run, however, growing awareness of identity theft among the general public means that your customers are demanding that their personal and financial information be secure. It is hoped that customers will understand if purchasing a vehicle takes longer than usual because you are working diligently to protect their information.

By Nov. 1, 2008, dealers will need to be able to prove they are doing their part to help counter identity theft by having a program in place to comply with the red flag regulation. Complying with the new regulation will not only safeguard your dealership from penalties and criminal action; it will help maintain your business's reputation as well.

Kelly Faehr is an executive specializing in audit, financial advisory, and consulting services for retail dealers with Crowe Chizek and Company LLC in Indianapolis. She can be reached at 317.706.2737 or kfaehr@crowechizek.com.

Banking Failures? What Should You Be Doing?

By Ronald Sompels, CPA

Business owners across the board are worried about the state of their financial institutions and what could happen to their cash and investments should these institutions fail. Author Ronald Sompels explores ways to safeguard your dealership's assets and prepare for the unexpected.

The news that IndyMac Bank was seized by U.S. regulators on July 11 has many business owners wondering how safe their assets are and what, if anything, they should be doing to protect them.

First, don't assume the worst. For all the recent bad news on Wall Street, only five Federal Deposit Insurance Corporation (FDIC)-insured local and regional banks have shut their doors so far this year.[1] The others that have failed have been a small fraction of the size of IndyMac, which held $32 billion in assets as of late March.[2] It has been 15 years since any bank larger

Under U.S. Treasury rules issued in 2005, we must inform you that any advice in this communication to you was not intended or written to be used, and cannot be used, to avoid any government penalties that may be imposed on a taxpayer.

than $10 billion in assets collapsed. William Isaac, chairman of the FDIC in the early 1980s, advised against widespread panic and noted that the number of bank failures so far is just a small percentage of the 3,000 failures that occurred in the 1980s.[3]

Although it does not yet appear to be time to get alarmed, it is always a good time to think about safeguarding and managing your assets. Here are a few things you should be doing.

Understand the health of your financial institution. There are several good financial institution rating services online, such as the one offered by BauerFinancial, that will provide you a rating on the health of the financial institution you use. This will allow you to assess the current health of your institution and others. In addition, these services can be used to monitor the status of your financial institution as conditions change. Armed with this information, you will be able to ask pointed questions of your financial institution representative.

Understand where your cash is invested. The majority of dealership owners use some sort of sweep arrangement to make sure all of their deposits are earning a return. You should understand how these sweep accounts are insured or collateralized. In many cases these accounts are invested in the commercial paper of the financial institution and are uninsured and uncollateralized.

Other dealers use “floor plan offset” accounts. In these instances, excess cash is offset against floor plan accounts to obtain a rate of return similar to what is being paid on the floor plan debt. It is our general experience that in most cases these funds are not actually used to pay down the floor plan debt but are, instead, deposited in separate deposit accounts. Dealers should check to determine if and how these separate accounts are insured or collateralized.

An alternative way to invest excess funds would involve daily monitoring of these funds and manually transferring them against lines of credit or other revolving instruments. This would limit exposure to uninsured deposits.

Have a backup plan. What would happen if the financial institution you were using did fail? Normally, it would take several days if not weeks to sort out how to access your cash and make arrangements with another institution to handle the relationship. It makes good sense to think about alternatives before the situation necessitates. It doesn’t hurt to have discussions, create relationships, and even have approved applications on file with another institution as a backup plan you could immediately implement if something unexpected happened.

We are going through some precarious financial times right now, and it is difficult to imagine what might happen next. One thing is certain: It never hurts to be prepared.

Ron Sompels is the executive-in-charge of the retail dealers group with Crowe Chizek and Company LLC in Tampa, Fla. He can be reached at 813.209.2401 or rsompels@crowechizek.com.

“Identifying Identity Theft: Complying With the New Red Flag Regulation”
[1] Federal Register, Volume 72, No. 217, Nov. 9, 2007, Rules and Regulations, **www.occ.treas.gov/fr/fedregister/72fr63718.pdf**, pp. 63718-63775.

“Banking Failures? What Should You Be Doing?”
[1] FDIC Bank Failures & Assistance, www.fdic.gov/bank/historical/bank/index.html.
[2] “IndyMac one of the largest bank failures in U.S. history,” *International Herald Tribune*, July 13, 2008, www.iht.com/articles/2008/07/13/business/indy.php.
[3] Ibid.