PHOTO: ©ISTOCKPHOTO.COM/SERDYNIA

Taking on the RED FLAG Rule

Recognizing the motivations behind this newest regulation will be key to understanding how the F&I department fits into this newest puzzle. F&I expert provides a road map to developing the required prevention program and tips on evaluating compliance vendors.

By Joe Bartolone

The days of just copying a driver's license and taking a verbal social security number are over with the finalization of the Red Flag Rule last October. Credit reports will need to be thoroughly scrutinized. Dealers will also need to know how to react when a red flag is raised, and will have to document each situation.

Dealers will also need to consider an identity verification solution for their sales process, as well as re-evaluate their spot delivery process and sales desk functions.

One of the most important decisions you'll need to make as a dealer is the approach you take to address the Red Flag Rule. You can take a minimalist approach and develop a program that meets the minimum requirements, or you can develop a program that addresses both the letter and the spirit of the rule.

The Red Flag Rule was born out of the Fair and Accurate Credit Transaction (FACT) Act. It was signed into law Dec. 4, 2003. It added several new provisions to the Fair Credit Reporting Act of 1970. Some of these requirements have already been enacted; some have already impacted your personal

life as well as your business.

One provision the FACT Act is responsible for is the one that allows individuals to request a free credit report annually. Another requires past victims of identity theft and active military personnel to be contacted any time a request to extend credit comes under their name.

The FACT Act also requires businesses provide victims of identity theft with copies of credit applications or transaction records used in the fraudulent deal. Other rules the FACT Act initiated were the disposal rule, address discrepancy notification requirements for credit-reporting agencies, and the truncation requirements for credit card and debit card numbers. I hope all of this sounds familiar to you and your business.

I think you can see where regulators are going with all of this. Identity theft is a big problem, and regulators are doing all they can to protect consumers.

The finalization of the Red Flag Rule (section 114 of the FACT Act) represents one of the final steps regulators are taking to protect consumer credit information. It requires financial institutions and creditors to establish reasonable policies and procedures for implementing an identity theft prevention program.

Regulators also sought to provide guidance on how users of credit reports respond to address discrepancies received from consumer-reporting agencies. This second component, which was also finalized last year, falls under section 315 of the FACT Act.

So, instead of looking at the Red Flag Rule as another government compliance program, consider marketing your commitment to thwart identity theft. Customers will definitely appreciate your efforts. Just remember the clock is already ticking, as the new rules went into effect on Jan. 1. Dealers should now have their sites on Nov. 1, the enforcement date of this newest regulation.

CREATING AN ID THEFT PREVENTION PROGRAM

Before you start searching for the finalized document on the Red Flag Rule, understand that it's 256 pages. Below is an outline to help you get started with your identity theft program. Just remember, there is a lot to consider with this newest regulation. That's why it's highly recommended that you seek legal advice. You should also seek out industry associations, as well as your lender partners.

PHOTO: ©ISTOCKPHOTO.COM/DAVE PLILBOSIAN

1 Developing a Written Program

What might be the biggest headache for dealers is developing a written program to combat identity theft. Just remember the program must contain "reasonable policies and procedures for detecting, preventing and mitigating identity theft." The first step under this heading is to identify areas that pose a risk to the business. So when it comes to F&I, dealers will need to identify the following:

- The types of accounts offered or maintained
- The methods it provides to open its covered accounts
- The methods it provides to access its covered accounts
- Previous experiences with identity theft

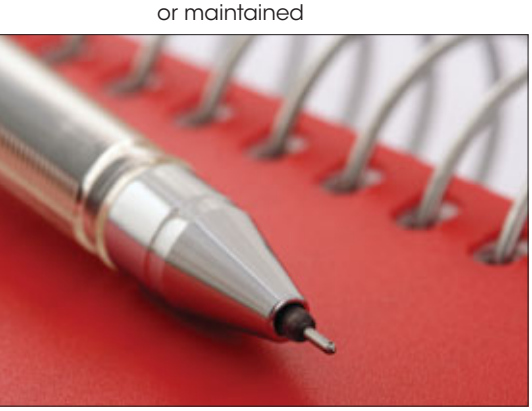

PHOTO: ©ISTOCKPHOTO.COM/EMILY2K

Dealerships will also have to determine sources of red flags relevant to their operation. Much of this can come from past experiences the dealership has had with identity theft. Dealer associations and legal advisors can also help identify other sources of red flags.

Dealerships will also need to identify when a red flag should be raised. This includes alerts, notifications or other warnings received from a consumer-reporting agency or a service provider, such as a fraud detection service. This also refers to suspicious documents (i.e., suspicious address change notice or personal identification documents) the dealership receives from a customer.

Notices from customers, identity theft victims or law enforcement are also indicators of a red flag.

2 Detecting Red Flags

Dealerships will also have to formulate policies and procedures F&I managers must adhere to on every transaction, which basically means an F&I manager doing his or her due diligence to verify the customer's identity. This will include such steps as collecting identifying information or verifying the validity of an address change notice.

PHOTO: ©ISTOCKPHOTO.COM/EMRAH TURUDU

3 Prevent and Mitigate Identity Theft

The program policies and procedures should also provide appropriate responses based on the risk posed when a red flag is raised. Responses could include contacting the customer, not completing a transaction and notifying law enforcement.

4 Program Updates

Dealerships will need to periodically update their program to reflect any new sources, trends or methods of identity theft. This means dealers will need to note how their program held up each time the dealership faced a red flag.

Dealers will also need to update their program to reflect any new procedures instituted at the dealership. And again, it's a good idea for dealers to remain in constant contact with their legal counsel, as well as state and local dealer associations to stay updated with any new developments related to identity theft.

PHOTO: ©ISTOCKPHOTO.COM/JOHN KOUNADEAS

5 Methods for Administering the Program

Aside from implementing the written program, dealerships will also need to designate an individual (typically someone at the senior management level) to oversee the program's development, implementation and administration. In fact, this could be the first thing a dealership does.

This individual is who dealership personnel will refer to whenever a situation related to the program arises. This is the person who will make the final call. He or she will also collect reports from staff about all matters related to the dealership's identity-theft program.

This person will also be required to collect reports from employees on the effectiveness of the program. This could include how the program addresses the risk of identity theft, service provider arrangements, significant incidents involving identity theft and management responses. This person will also be responsible for recommending and implementing changes to the program.

PHOTO: ©ISTOCKPHOTO.COM/EMRAH TURUDU

6 Other Legal Requirements

A dealership's written program will also need to include requirements for extending credit to a customer despite the detection of a fraud or active duty alert. This is important for dealers operating in areas housing military personnel. Dealerships will also need to implement any requirements for sending consumer reporting agencies corrected or updated information about a customer.

FINDING THE RIGHT SOLUTION

The Red Flag Rule will definitely be a hot topic at this year's National Automobile Dealers Association (NADA) convention. Here are a few questions to help you find the right solution.

- What element(s) of the Red Flag Rule does your solution address? *Total or partial solution*
- What training solutions are included with your solution? *(e.g., onsite, online, other types of media)*
- How does your solution identify and detect red flags? *You want to know how much of the process is manual, electronic, and whether the solution can be utilized with an existing technology.*
- How will your solution help prevent and mitigate identity theft? *What part of the solution is subjective and based on statistical analysis? And what part offers true identity verification? Does the solution offer out-of-wallet challenge questions, or information typically not found in a person's wallet?*
- What is the cost of your solution? T*echnical solutions can be transaction-based or based on an annual no-limit fee. Consulting services are generally based on a daily rate plus expenses. Attorney's fees could be hourly or daily.*
- Do you offer a template solution for the Red Flag program? *A template solution is easily customizable and more cost-effective than custom solutions.*
- How long will it take to implement your solution? *In addition to time, consider how intrusive the implementation of the solution may be to your daily operations.*

PHOTO: ©ISTOCKPHOTO.COM/JANNE AHVO