

Best Practices for Developing Your Red Flags Rule Program



Mark O'Neil, is CEO of DealerTrack Inc., the nations largest automotive finance network that also provides innovative products to over 22,000 dealers to help them sell, finance, fund and increase their level of compliance.

MOneil@AutoDealerMonthly.com

Most of you reading this are probably aware of the Federal Trade Commission's new Red Flags Rule which requires all dealerships to "develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts." Compliance with the new Rule is mandatory by Nov. 1, 2008. Your program must be appropriate to the size and complexity of your dealership and the nature and scope of your activities, and your board of directors must approve the initial program.

Many dealerships have not started drafting their program. If your dealership is procrastinating on developing your program, or doesn't know where to begin, the following tips and best practices can help you craft and maintain a Red Flags program that will meet FTC requirements and protect your dealership.

Identify Your Red Flags

The Rule lists 26 potential red flags that may signal identity theft, but not all of them will apply to your dealership. Your first step in drafting your program is to review these red flags and determine which are relevant to your dealership. To

identify other red flags, talk to your fellow dealers and big-ticket retailers near your dealership. Your local law enforcement may also be able to tell you about behaviors they've seen identity thieves exhibit.

Detect and Respond to Red Flags

Next, you need to adopt a process to detect any of your red flags in each customer credit transaction. Three excellent ways to do this are:

- 1) Review the customer's identification documents, such as their driver's license or other photo ID, for inconsistencies or tampering.
- 2) Review the customer's credit report for things like address discrepancies, fraud alerts and recent unusual patterns of activity.
- 3) Use an electronic identity verification service to compare the customer's information against databases of fraudulent or irregular information to identify suspicious Social Security numbers, addresses and phone numbers linked to fraud and other problems.

If your detection process suggests a possible red flag, have a series of follow-up questions for each red flag in your program. Then, after asking these questions, if you are still uncertain about the customer's identity, consider using "out-of-wallet"

questions available from identity verification services. These questions allow you to ask the customer things that are not likely to be known from a credit report or stolen wallet, and that only the real customer would know. You can also ask questions about old items on the customer's credit report like: "Who was your car loan with in 2003?"

Establish a process to gather this information (for most customers, the process should only take a few minutes); then escalate to a senior program officer any remaining concerns suggesting unresolved red flags or an identity thief. This senior officer can also speak with the customer, obtain and ask more out-of-wallet questions, or seek additional verification documents such as a utility bill or a passport.

Whether you decide to proceed with the transaction or not, make sure that you document every step of your process to show that you followed established procedures. Safeguard that information the same way you safeguard customer information under your Safeguards and Disposal programs.

Update Your Program

Because identity thieves are constantly finding new ways to steal information, identity theft protection is not a static process. The Rule requires that you assess and update your program using reports made by participating employees at least once every year. However, it is a best practice to update your program more frequently as you have experience with potential identity thieves and learn more about identity theft risks.

The Red Flags Rule does not require you to get the customer's identity right every time, but it does mandate that you establish a program appropriate to the size, complexity and activity of your dealership, and that you follow your procedures consistently. Having written policies and procedures to do this will make your process for verifying customer identities systematic and efficient. Follow the process the same way for every customer.

Train your Staff and Research Solutions

Once you have your program in place, you must train your employees to understand your red flags and how to perform their specific obligations under your program. Accomplishing this may include a combination of group training on your program, individual training for specific activities, and incorporating an electronic identity verification tool that can quickly identify suspicious information. Remember that whenever you update your program, additional training will be necessary as well.

Most dealerships already scrutinize a customer's identity by doing things like checking a photo ID and examining information on a credit application to detect discrepancies with credit bureau data. So although establishing a written program will take some time, much of what it must include, you already know or do. With technology solutions like identity verification services to help you identify possible red flags and helpful compliance guides, you can more easily develop processes and procedures that will keep your dealership compliant. **ADM**