

Is your Compliance Policy Compliant?

by : JR Wilson

By now you have probably heard or read about the newest federal regulation, called the Red Flag Rule. Effective this year, it's the last piece of the Fair and Accurate Credit Transaction Act of 2003 (FACTA) and requires dealers to develop an identity theft prevention program (ITPP) that identifies and evaluates any discrepancy in information used when someone applies for credit. Although the multi-agency federal board provided 26 examples of "red flags" that could indicate identity fraud such as a bureau fraud alert, a DOB that doesn't match the applicant's appearance, a recent address change, high number of recent bureau inquiries, dealers are still left without a full policy that eliminates identity fraud and brings them into compliance.

The requirement, and intent, of the ITPP is to "detect, prevent and mitigate identity theft," yet with only the list of 26 "red flags" as a guideline, each creditor or financial institution is left without the proper tools to do so. And in the event they are successful in identifying one of these potential red flags, they are left with the cumbersome problem of trying to figure out how to interpret it to mitigate the risk of identity fraud. This will create a misunderstanding of the regulation and could result in inconsistent degrees of compliancy and protection. So can you have an ITPP and still be exposed to, and responsible for identity fraud? The answer, unfortunately, is yes.

Though they seem intuitive and easily applied to an identity theft prevention policy, most of the "red flags" outlined by the board aren't as effective as they seem. Let's look at some of these and how useful they are within an ITPP (on a scale of one to 10):

- **Fraud alert:** These appear *after* someone has realized he or she is an identity fraud victim. If this has appeared in a credit file, you can be assured that the thief has already moved on to the next identity, leaving the real person to clean up the mess. *ITPP significance: 0*
- **New address:** A new address may indicate an attempt to forward mail to avoid detection—or it may just be a new, valid address. How do you confirm a legitimate address change? Copy of a utility bill? This can be forged as well. *ITPP significance: 2*
- **Recent bureau inquiries:** A lot of inquiries confirm someone's attempt to obtain credit, but when shopping for a car, that means obtaining credit...right? If there are multiple inquiries, it could indicate a 'smash and grab' fraudster but can also indicate normal consumer shopping patterns. *ITPP significance: 2*
- **A tampered-with driver's license:** Why would a thief tamper with a driver's license when he can order a novelty license online that looks exactly like the real thing? Also, how are you going to examine a license on an Internet deal? (Besides that, how many salespeople even look at the driver's license?) I intentionally gave my expired driver's license to a salesperson once to see if he would notice. He didn't, and I went on the test drive anyway. Every fraudulent deal I've seen has included a counterfeit driver's license. *ITPP significance: 0*
- **Phone number doesn't correlate with address, is a cell phone or VOIP number:** With the rising cost of traditional land lines there are plenty of people who have only a cell phone. I have a friend who has lived in Dallas for two years but has kept his Atlanta cell phone number because that's the number all his friends and clients have. Someone can use a pre-paid (i.e.: disposable) cell phone but technology is not available to detect the difference between that and a regular cell phone line. *ITPP significance: 0*
- **SSN has been reported deceased:** This used to be the number-one method of identity theft but since bureaus started including this alert, thieves have abandoned this approach. However, I recently learned of a deal where the co-buyer's SSN was reported deceased. Both the finance manager and the bank missed the alert. *ITPP significance: 8 (but this method is now unlikely to be used by a thief and still needs to be detected by the FIM)*

In the end, these red flags can be an indicator of identity fraud, but they can also be signs of normal consumer spending habits. Unfortunately, there is no way to determine the difference without the proper tools and training. And if you leave

the interpretation of these red flags in the hands of your employees, you will increase your liability. That's because each person will evaluate the risks differently based on their own experiences. The reality is once managers have to jump through hoops to verify information on one deal that doesn't turn out to be fraudulent, they will likely sign off without verification the next time the issue arises. But failing to implement a comprehensive identity theft prevention policy or relying on employee interpretation of the red flag risks using the list as a guideline alone could lead to the circumvention of the policy altogether.

If you fail to proactively authenticate each applicant's identity, and only rely on the 26 red flags, you will create 1) a program that leaves you at risk, 2) a burden on the dealership staff with complicated and unnecessary manual verification, 3) a program that quickly diminishes in effectiveness and quality, and 4) a policy that is not compliant.

If you're still not convinced, look at the facts. Among the fraudulent deals I've examined, all of them included a counterfeit driver's license, a counterfeit insurance card, a forged signature, no bureau fraud alert and a legitimate address. Today's technology is sophisticated; thieves can and do procure perfect replicas of driver's licenses and insurance cards via the Internet every day. When they present these official-looking documents, they don't raise concern and definitely fail to raise any red flags. In fact, it sounds like any normal deal you handle every day, doesn't it? This is exactly why you cannot rely on only the FACTA-inspired red flags and need to include a definitive identity verification policy in your ITPP.

There are several different approaches to an ITPP solution and there are varying degrees of technology available to enhance your program. The options include basic fraud alerts, statistical analysis interpretation (and corresponding scoring systems) of the red flags, electronic driver's license verification and positive identity verification. The manual requirements of your ITPP will differ based on which technology you decide to utilize as part of your program. The more comprehensive the technology, the less complicated the manual process becomes; meaning you can, in fact, fight the thieves' technology with your own.

As with any regulation, there will be many different interpretations, and, unfortunately, many dealers who will take a minimalist approach in order to save a few bucks. It is a stance you simply must avoid. If you do not include a true identity verification process into your ITPP, and I'm not just talking about looking at the driver's license or getting a fingerprint, you will leave yourself wide open. Aside from the risk of identity theft, you will be at risk for non-compliance with the law, a charge-back from the bank, and possibly a lawsuit.

J.R. Wilson is an expert on identity fraud and the president of PatriotDealer.com, which provides identity verification and compliance services to dealerships. Wilson has spoken at all three AAISP workshops on the topic of identity fraud in the retail automotive industry.