



Is Your Dealership Red Flag Compliant?

The Red Flags Rule, very simply put, was designed by the Federal Trade Commission (FTC) to help organizations detect and prevent identity theft that may arise during the lending process. Your dealership is required by law, to establish a formal, written identity theft detection and response program to protect your dealership and your customers. As your business office, Priority One has created and implemented a program in accordance with the Red Flag Rules and if you do not already have a program in place at your dealership, you may find it helpful to follow the steps that we used when designing our program.

Step 1: IDENTIFY RELEVANT RED FLAGS

It is important to understand exactly what the FTC defines as a "Red Flag." A Red Flag is a pattern, practice or specific activity that indicates the *possible* existence of identity theft. The Red Flags Rule contains a list of 26 potential red flags, though chances are not all of them will apply to your dealership. Individual compliance obligations do not follow a one-size fits all formula; the program is to be tailored to your dealership's level of risk. At Priority One, we have identified 12 of the 26 that apply to the credit applications we receive. For a list of the 26 red flags, visit http://www.bankinfosecurity.com/articles.php?art_id=932.

Step 2: DETECT AND EVALUATE RED FLAGS

Your dealership must set up policies and procedures to detect and respond to red flags. A red flag could include suspicious or altered documents provided by your customers, inconsistencies between information on the credit application and the customer's photo ID, or warnings from a fraud detection service. Inconsistencies don't necessarily serve as proof of identity theft or fraud but should serve as a red flag signaling your staff to conduct additional verification of the customer's identity. Priority One helps you stay compliant by running all applications through our proprietary system which scans the customer's credit bureau and compares it to the application instantly identifying any fraud alerts, credit freezes and discrepancies in the customer's name, address, social security number and date of birth. If a discrepancy is found and determined to be a potential red flag, Priority One will immediately contact the customer for additional information and will advise your staff of the extra steps to be taken prior to delivery to verify the customer's identity.

Step 3: CREATE A POLICY AND PROCEDURE MANUAL

Regardless of the Red Flag policies and procedures your dealership chooses to incorporate, a written program must be created, implemented and updated on a regular basis. The written manual should include the red flags that apply to your dealership, how you will identify those red flags, what steps your staff should take when a red flag is detected and what supporting information is required to verify identity. Priority One employees are required to follow set policies and procedures once any red flags are detected and identified. Our employees must perform additional due diligence on the transaction in order to verify the customer's identity by following our standard operating procedures before the closing package is sent to your dealership. For example, if the address provided by a customer does not match the address on the credit bureau, the customer would be asked to provide verification of their current address in the form of a recent utility bill.

(continued)

At Priority One, we don't just stop there. Your dealership's and customer's information is protected through a number of levels of security. Entry to our building is limited only to those with a coded access card. Customer files are not permitted to be taken off premises and all sensitive information to be thrown away is placed in locked bins and shredded. Computers and individual programs are locked and accessible only with a unique username and password and our proprietary software has various levels of security built in limiting access to dealership and customer information based upon your position. Communication between our lenders and Priority One utilizes various industry accepted encryption methods and our network has extensive firewall, SPAM and virus protection as well as an intrusion detection system. Your dealership should conduct annual security audits to ensure your systems have all software updates/patches and no processes have been compromised.

Step 4: TRAIN AND UPDATE PROGRAM

Your Red Flags program must include a staff training plan as well as a regular review of the policy to provide updates due to industry changes, trends, changes in your operations or new sources of identity fraud. Priority One reviews our Red Flags program annually and conducts frequent audits to ensure procedures are being followed. New employees receive a written overview of our Red Flags policy and are required to view a training video on the Red Flags Rule. Additionally, we conduct annual refresher courses to all staff.

Finally, once your dealership has created a written program, assign an individual responsible for overseeing and implementing changes to the program. This person should be someone at the senior management level and if possible, part of the team that created your dealership's original program.

The creation of the Red Flags Rule and your lawful responsibility to create a compliance program is very important for your customer's and dealership's protection against identity theft. Following these four simple steps can help you decipher the requirements of the Red Flags Rule and guide you through implementing a program within your dealership. For additional information on the Red Flags Rule, check out <http://www.ftc.gov/redflagsrule> or for more information on how Priority One helps keep your dealership compliant, contact Lorraine Mariotti, VP of Lending at lmariotti@p1fs.com.