What are Red Flag Rules?

The Red Flag Rules:
- Are enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration.

- Set out how certain businesses and organizations must develop, implement and administer their Identity Theft Prevention Program.

- These rules have been in effect since January 1, 2008.

"As many as nine million Americans have their identities stolen each year. Identity thieves may drain their accounts, damage their credit, and even endanger their medical treatment."

-Federal Trade Commission, "Fighting Fraud with the Red Flag Rule"

Who Must Comply With these Rules?

Financial Institutions and Creditors must comply.

- Jack Byrne Ford is a creditor because we, "regularly defer payment for goods or services or provide goods or services and bill customers later."

- The definition further describes "covered accounts." These are accounts where there may be a "foreseeable risk of identity theft." This is particularly true if the account can be accessed remotely, such as through the Internet or telephone.

Jack Byrne Ford Covered Accounts Include:

- Consumer vehicle installment sale contracts
- Consumer vehicle leases
- Business vehicle installment sale contracts
- Business vehicle leases
- Consumer Parts and Service Charge
- Business customer Parts and Service Charge
- Dealership employee Parts and Service Charge
- Consumer Daily Rental Car Charge
- Business Daily Rental Car Charge

Compliance is a Four-Step Process

Step 1: Identify Relevant Red Flags
Step 2: Detect Red Flags
Step 3: Prevent and Mitigate Identity Theft
Step 4: Update your Program

Step 1: Identify Red Flags

There are five different categories for identifying red flags:

1. Notifications and Warnings from Credit Reporting Agencies

2. Suspicious Documents

3. Suspicious Personal Identifying Information

4. Suspicious Covered Account Activity or Unusual Use of Account

5. Alerts from Others

Category 1: Notifications and Warnings from Credit Reporting Agencies:

1. Report of fraud accompanying a credit report;

2. Notice from a credit agency of a credit freeze;

3. Notice from a credit agency of an “active duty alert”;

4. Receipt of address discrepancy in response to a credit report request; and

5. Indication from a credit report of activity inconsistent with an applicant’s usual pattern or activity.

Category 2: Suspicious Documents:

Almost all departments of Jack Byrne Ford with covered accounts work with some form of documentation. These documents may include credit applications for vehicle sales, applications for employment, taxation and revenue documentation, driver’s license and change of address requests. Red flags include:

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document;

3. Other document with information that is not consistent with existing customer/employee information; and

4. Application that appears to have been altered or forged.

Category 3: Suspicious Personal Identifying Information:

When dealing with individuals at Jack Byrne Ford, proper identifying information is needed. This may include a driver's license or passport. On the phone, employees should verify birth date or other personal information. Suspicious information can include:

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. The social security number has not been issued or is listed on the Social Security Administration's Death Master File;

3. A person fails to provide complete personal identifying information on an application when reminded to do so; and

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address

Category 4: Suspicious Account Activity or Unusual Use of Account

Any of the following should be considered a Red Flag.

1. Change of address on account followed by a request to change the customer's name;

2. Payments stop on an otherwise up-to-date account;

3. Mail sent to a customer is repeatedly undeliverable although there is account activity;

4. Notice from a customer that they are not receiving a statement;

5. Notice to Jack Byrne Ford that the account has unauthorized activity;

6. Unauthorized access to or use of customer account information

Category 5: Alerts from Others:

An obvious Red Flag occurs whenever notice is given to Jack Byrne Ford from a Customer, identity theft victim, law enforcement agency or other person that Jack Byrne Ford has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Once you've identified what constitutes a possible Red Flag, what's the next step?

Step 2: Detect Red Flags

Now that your department knows what a Red Flag looks like, it's time to come up with procedures to detect Red Flags in your own area. Two areas of particular concern are:

1. Before opening the account, obtain, inspect, and photocopy the consumer's (or business customer's representative's) current driver's license or other government-issued photo identification and, for a business entity customer, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

   A. Review the identification document for signs of alteration or forgery.

   B. Compare the photo and physical appearance information on the identification with the consumer's in-person appearance.

2. Before opening the account, obtain customer's signed credit application that includes, at a minimum, the customer's name, date of birth (or of formation, if a legal entity), residential or business street address (or of principal place of business if a legal entity), and Social Security or Taxpayer Identification Number.

A. Review the credit application for signs of alteration or forgery.

B. Review the address and other information on the credit application for consistency with information provided in the consumer report.

C. Review the information on the credit application for completeness.

3. Before opening the account with a consumer, obtain a consumer report.

A. Check for a fraud or active duty alert.

B. Be alert for notice of a credit freeze from the credit reporting agency.

C. Check for a notice from the credit reporting agency of an address discrepancy.

D. Review the report for activity inconsistent with the history and usual pattern of activity of Dealership customers generally.

E. Review the address and other information on the credit application for consistency with information provided in the consumer report.

F. Review any alerts or notifications of unusual activity, conditions, or events issued by the credit reporting agency or otherwise provided with the consumer report.

4. Make all finance and sales desk personnel aware of notifications of potential identity theft attempts.

5. Proceed with account opening with the assumption that the execution of documents and delivery of the vehicle will occur on-site, at Dealership's facility. Be alert to any effort by the customer to request or steer the transaction toward having the co-buyer or co-lessee sign documents off-site.

6. Verify through a source other than the representative himself or herself (such as by contacting the business customer's office) that any representative of a business customer has authority to act on behalf of that business customer.

Step 3: Prevent and Mitigate Identity Theft

In the event we detect any identified Red Flags, these individuals should discuss the situation with his or her supervisor who will take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

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

To protect consumer information we will:

- Secure customer information at all times. Customer information is not to be left where others can steal that information.
- Ensure complete destruction of paper documents and computer files containing customer account information when a decision is made to no longer maintain such information.

- Ensure office computers with access to account information are password protected.

Step 4: Update the Program

When necessary the program will be updated since our environment changes constantly. Technological advances and the ability to conduct most business online makes it imperative that individual departmental policies and procedures be reviewed and updated periodically.

Know your environment.
Know your customers.
Know your risk

Where Can I Get More Information?

Federal Trade Commission's (FTC) Red Flags Rule Website:
http://ftc.gov/redflagsrule