Jack Byrne Ford & Mercury Identity Theft Program (ITPP)

PART ONE—BACKGROUND

1. Effective Date

All affected employees of Jack Byrne Ford & Mercury ("Dealership") must comply with the terms of this policy as instructed by their respective supervisors but no later than May 1st 2009

2. Purpose and Policy

It is Dealership's policy to develop, implement, and maintain a comprehensive Identity Theft Prevention Program ("ITPP" or "Program") to detect, prevent, and mitigate identity theft in connection with the opening of all covered accounts or, if there are cases where Dealership has retained a covered account, in connection with existing covered accounts. For purposes of this Program, and the Red Flags Rule discussed below, "identity theft" occurs when a person commits or attempts to commit fraud using identifying information of another person without authority.

This Program is intended to comply with the requirements of the Identity Theft Rules (16 C.F.R. part 681), issued by the Federal Trade Commission (FTC) in compliance with Sections 114 (Red Flags Rule) and 315 (Address Discrepancy Rule) of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), 15 U.S.C. 1681m(e) and 15 U.S.C. 1681c(h).

No part of this Program or related policies and procedures should be interpreted as contravening or superseding any other applicable legal and regulatory requirements. This Program and its related policies and procedures reflect Dealership's good faith efforts to comply with applicable law and reduce the potential for identity theft. They do not represent warranties, representations, or contractual obligations in favor of any person or group.

3. Responsibilities and Management

Under this Program, the board of directors of Dealership has the authority and responsibility to:

- Approve this ITPP

The Compliance Officer, a member of Dealership's senior management, has been designated to supervise the overall management of the ITPP. The Compliance Officer has the authority and responsibility to:

- Oversee and manage the development, implementation, and administration of the ITPP
- Assign specific responsibility for the Program's implementation, including but not limited to appointing, supervising, and managing the activities of the Program Coordinator and others having specific responsibility related to the ITPP
- Review reports prepared by staff regarding compliance by the Dealership with the Red Flags Rule and this Program
- Approve material changes to the Program as necessary to address changing identity theft risks
- Exercise management control as

necessary to ensure that all relevant Dealership operations and employees make compliance with this Program an integral part of regular operations

The Program Coordinator has been designated to manage and coordinate the ITPP under the supervision and management of the Compliance Officer. As deemed necessary by the Compliance Officer, such as at the inception of this Program, the role of Program Coordinator may be undertaken by a team of employees designated by the Compliance Officer.

PART TWO—PROGRAM DEVELOPMENT AND ASSESSMENT

Part Two reflects the process used for development and periodic assessment of Program, including identification of covered accounts and relevant Red Flags, methods of detecting relevant Red Flags, and means of response when relevant Red Flags are detected.

4. Range of Accounts

The Red Flags Rule requires Dealership to initially (and periodically thereafter) determine whether it offers or maintains "covered accounts" as defined by the Rule. To do so, Dealership will evaluate each account offered or maintained by Dealership to determine if it is a covered account.

For purposes of this Program and the Red Flags Rule, an "account" can be defined as any extension of credit to a consumer (i.e., for personal, family, or household purposes) or business to obtain a product or service, except those extensions of credit not involving a continuing relationship. An example of a transaction that would not constitute an account under the regulations because it lacks a continuing relationship would be the acceptance of a personal check for a simple purchase. However, the Red Flags Rule applies to the opening of an account as well as account maintenance, so an account may exist in situations where Dealership extends credit but then assigns the credit contract to a third party.

5. Risk Assessment

The definition of covered account requires some types of accounts, such as business accounts, to be evaluated to determine if they pose a reasonably foreseeable risk of identity theft warranting their treatment as covered accounts. This evaluation is referred to as a "Risk Assessment." The Rule also requires the Dealership to periodically identify relevant Red Flags for the covered accounts it offers or maintains. In identifying relevant Red Flags, the Dealership must also consider risk factors applicable to the covered accounts.

The Risk Assessment for determining whether certain accounts are covered accounts is similar to the Risk Assessment to be used in identifying Red Flags. Therefore, in connection with the periodic identification of covered accounts and identification of relevant Red Flags, the Dealership will conduct a Risk Assessment of its accounts and, at a minimum, will take the following factors into consideration:

- The types of accounts Dealership offers or maintains
- The methods Dealership employs to open its accounts
- The methods Dealership employs to access its accounts
- Dealership's previous experiences with identity theft

Account Identification and Risk Assessment Worksheets

In conducting the Risk Assessment, the Program Coordinator may use the Account Identification and Risk Assessment Worksheets attached to this Program.

The Account Identification and Risk Assessment Worksheets shall be prepared

to list individually each type of account offered or maintained by the Dealership on a department-by-department basis (e.g., new- and used-car sales departments, parts and service, etc.) and by customer type (e.g., consumers, local businesses, fleet businesses, vendors).

The Risk Assessment shall be evaluated and used also in consideration of the size and complexity of Dealership and the nature and scope of its activities.

6. Identification of Covered Accounts

It is Dealership's policy to determine periodically whether it offers or maintains covered accounts as defined in the Red Flags Rule and to identify any such covered accounts.

A covered account is defined as (1) an account that Dealership offers or maintains primarily for personal, family, or household purposes and that involves or is designed to permit multiple payments or transactions, such as a consumer vehicle installment sale or lease contract; and (2) any "other account" that Dealership offers or maintains (such as a business installment sale, lease, or parts open account) for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Dealership from identity theft, including financial, operational, compliance, reputation, or litigation risks.

As such, it is the policy of Dealership to conduct a periodic Risk Assessment to determine whether it offers or maintains such "other accounts," taking the following factors into consideration:

- The methods Dealership provides to open its accounts
- The methods Dealership provides to access its accounts
- Dealership's previous experiences with identity theft

For the foregoing purposes, the Risk Assessment referred to in Section 5 of this Program may be used.

7. Identification of Relevant Red Flags

It is Dealership's policy to periodically identify relevant Red Flags for the types of covered accounts it offers or maintains by considering appropriate risk factors, categories of Red Flags, and other sources of Red Flags.

Risk factors

In identifying the relevant Red Flags for the types of covered accounts offered or maintained by Dealership, the Risk Assessment referred to in Section 5 of this Program shall be taken into consideration. The following factors will be considered:

- The types of covered accounts Dealership offers or maintains
- The methods Dealership employs to open its covered accounts
- The methods Dealership employs to access its covered accounts
- Dealership's previous experiences with identity theft

Categories of Red Flags

In identifying the relevant Red Flags for the types of covered accounts offered or maintained by Dealership, the following categories of Red Flags shall be taken into consideration. Where appropriate, Red Flags from these categories shall be

included in the Program:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- The presentation of suspicious documents
- The presentation of suspicious personal identifying information, such as a suspicious address change
- The unusual use of, or other suspicious activity related to, a covered account
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor

Sources of Red Flags

In identifying the relevant Red Flags for the types of covered accounts offered or maintained by Dealership, the following sources of Red Flags shall be taken into consideration. Where appropriate, Red Flags from these sources shall be included in the Program:

- Incidents involving identity theft Dealership has experienced
- Methods of identity theft Dealership has identified that reflect changes in identity theft risks
- Applicable supervisory (regulatory) guidance, including but not limited to the Example Red Flags contained in Supplement A to Appendix A of the Red Flags Rule

ID Theft Experience and Awareness Log. The Program Coordinator shall create and maintain a log of all incidents involving identity theft Dealership experiences and methods of identity theft Dealership has identified that reflect changes in identity theft risks.

Red Flag Identification, Detection, and Response Worksheets

The Red Flag Identification, Detection, and Response Worksheets attached to this Program shall be used in the periodic identification of relevant Red Flags and the development of policies and procedures for the detection of relevant Red Flags and the appropriate response to detected Red Flags.

The first Red Flag Identification, Detection, and Response Worksheet attached to this Program lists (and calls for the evaluation for possible inclusion in this Program of) the 26 Example Red Flags included in Supplement A to Appendix A of the Red Flags Rule as well as other potential Red Flags. For periodic assessments, the Worksheet shall be revised to include any additional Red Flags from any of the sources of Red Flags referred to under the heading “Sources of Red Flags” above. Other potential Red Flags from other sources shall also be included on the Worksheet.

Each potential Red Flag included on the attached Worksheet will be evaluated in light of the following: the Risk Assessment for covered accounts; the categories and sources of Red Flags; Dealership’s size, complexity, and nature and scope of its activities; Dealership’s existing identity theft prevention policies; the cost and availability of establishing methods to detect the Red Flag; and whether in light of these considerations and other relevant facts it would be reasonable and appropriate for the Dealership to include the Red Flag in the ITPP.

8. Identification of Methods to Detect Relevant Red Flags

The policy of Dealership is to detect Red Flags incorporated into this Program by appropriate means, such as: (a) obtaining identifying information about, and verifying the identity of, a person opening a covered account and (b) where Dealership maintains a covered account after it is opened, authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

To develop more detailed policies and procedures for detection of relevant Red Flags and verification of identity, the Red Flag Identification, Detection, and Response Worksheets attached to this Program shall be completed by the Program Coordinator.

In addition, the existing policies and procedures of Dealership respecting verification of identity shall be considered in establishing the policies and procedures of Dealership regarding methods to detect relevant Red Flags and verify identity. The Red Flag Identification, Detection, and Response Worksheets attached to this Program shall be completed to include information about these existing policies and procedures.

Once each Worksheet is complete, the detection methods identified in the specific sections of the Worksheets and within each Red Flag template may be arranged together in the form of a list, with duplicates removed. This list may then be used to evaluate the appropriate procedures to be used by Dealership to detect relevant Red Flags.

PART THREE—RED FLAG IDENTIFICATION, DETECTION AND REPSONSE

Part Three reflects policies and procedures to be followed by Dealership in the ordinary course of business in opening and, if and when applicable, maintaining covered accounts.

9. Covered Accounts Offered or Maintained by Dealership

Based on the Risk Assessment and further review of Dealership's activities respecting its accounts, and subject to revision based on periodic review and updating, Dealership offers or maintains the following types of covered accounts:

- *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*

10. Relevant Red Flags Incorporated into this Program

After consideration of the Risk Assessment, including completion of the Red Flag Identification, Detection, and Response Worksheets, the following relevant Red Flags are hereby incorporated into this Program:

- *A fraud or active duty alert is included with a consumer report.*
- *A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.*
- *A consumer reporting agency provides a Notice of Address Discrepancy.*
- *A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as: (a) a recent and significant increase in the volume of inquiries; (b) an unusual number of recently established credit relationships; (c) a material change in the use of credit, especially with respect to recently established credit relationships; or (d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.*
- *Documents provided for identification appear to have been altered or forged.*
- *The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.*
- *Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.*
- *An application appears to have been altered or forged, or gives the appearance of having been destroyed*

and reassembled.

- *The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.*
- *Personal identifying information provided by the customer is inconsistent when compared against external information sources used by the dealership. For example, the address on the credit application does not match any address in the consumer report.*
- *Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, the credit application reflects that the customer owns his home but the residence address reflects an apartment number.*
- *Personal identifying information provided by the customer is associated with known or suspected fraudulent activity as indicated in alerts or warnings received by the creditor from a consumer reporting agency.*
- *Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated in alerts or warnings received by the Dealership from a credit reporting agency. For example: (a) the address on an application is fictitious, a mail drop, or a prison; or (b) the phone number is invalid, or is associated with a pager or answering service.*
- *Dealership is notified by a customer, a financial institution with which Dealership does business, victim of identity theft, a law enforcement authority, or any other person that an individual who may attempt to open an account with Dealership is engaged in identity theft.*
- *A customer seeks to execute a vehicle credit sale or lease and take delivery of the vehicle off-site—at a location other than the Dealership's facility.*
- *A co-buyer or co-lessee is included in the vehicle credit sale or lease but is not present at the Dealership facility to sign the contract or lease.*

11. Methods for Detection of Relevant Red Flags

Based on review of the Red Flag Identification, Detection, and Response Worksheets and other relevant information, Dealership will employ the following methods of verification of the identity of persons opening a covered account and of detection of the Red Flags incorporated into this Program:

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, using available information on forgery detection, if any, supplied by the agency that issues the identification*

document.

   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.*

12. Policy and Procedure for Responding to Detected Red Flags

General Policy When Relevant Red Flags Are Detected

It is the policy of Dealership to respond appropriately to relevant Red Flags that are detected in a manner intended to prevent or mitigate identity theft, commensurate with the degree of risk posed.

In determining an appropriate response, Dealership will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records with Dealership or a third party.

Appropriate responses by the Dealership may include:

- 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

Determining the appropriate response in any particular situation involves consideration of several factors. Therefore, in cases where the general and specific response procedures set forth below result in the conclusion that there is reasonable basis to believe identity theft may be involved, the Program Coordinator and appropriate Dealership manager shall work cooperatively to determine the appropriate response.

General Response Procedures when a Red Flag is Detected

While an important warning sign of possible identity theft, the detection of a Red Flag does not necessarily mean identity theft is involved. Many detected Red Flags can be resolved by the exercise of diligent investigation and verification. The purpose of this general response procedure is to allow detected Red Flags to be cleared, where appropriate, by dealership employees involved in the opening of covered accounts.

If a Dealership employee engaged in opening an account for a customer detects one or more Red Flags, the employee shall notify his or her manager and, before continuing to open the account, shall do the following:

- Conduct a reasonable investigation concerning the Red Flag(s) detected, including obtaining additional information from the customer and third-party sources, and
- Determine whether the Red Flag(s) detected or other circumstances require a specific response under the section below entitled “Specific Response Procedures.”

The account shall not be opened unless the manager determines that (a) the investigation adequately assessed the risk presented; (b) all specific response requirements, if any, have been fully and properly completed; and (c) there is no reasonable basis to believe that identity theft is involved. If this determination is not made, the manager shall advise the Program Coordinator of all of the circumstances and will work with the Program Coordinator to identify and undertake any other appropriate response consistent with applicable law and the policy of Dealership set forth at the beginning of this section.

In addition, if Dealership learns before assigning an account to a financial institution that the account resulted from identity theft, Dealership will refrain from assigning that account and the Program Coordinator shall work with the appropriate Dealership manager to properly respond.

Specific Response Procedures if Specific Red Flags are Detected

When certain Red Flags are detected or other related circumstances are identified, specific response procedures may be required by applicable law or policies and procedures adopted by Dealership.

Detection of the following Red Flags requires the specific response procedures to be followed as indicated below:

Fraud or Active Duty Alert Appears on a Consumer Report. *Section 605A of the FCRA, 15 U.S.C. 1681c-1(h), requires a creditor to take certain steps before extending credit, increasing a credit limit, or issuing an additional card on an existing credit account. To comply with this law and to minimize the potential for identity theft, follow the procedures below:*

1. *Do not open the account until and unless the following verification procedures are completed:*
   - *A. Contact the consumer using the telephone number or other means of contact stated in the alert, if any, and obtain authorization to proceed with opening the account.*
   - *B. Take all other appropriate reasonable steps to verify the consumer's identity and to confirm that the application to open the account was not the result of identity theft.*
   - *C. Obtain and verify governmental photo identification and follow the other requirements of Dealership's ITPP.*
   - *D. Prepare and sign a written acknowledgment specifying that verification procedures have been completed and detailing how each of the above steps was completed.*

Notice of Address Discrepancy Appears on a Consumer Report. *Follow the Notice of Address Discrepancy Policies and Procedures contained in this Program.*

Credit Freeze. *Do not open the account unless the consumer causes the freeze to be lifted and a credit report is obtained. Verify the consumer's identity and confirm that the application to open the account was not the result of identity theft.*

Documents provided for identification appear to have been altered or forged.

OR

The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification. *Do not open the account unless a reasonable and verified explanation that is not indicative of identity theft or forgery is provided that explains the appearance of alteration or forgery and the customer provides at least one additional non-forged/non-altered form of government-issued photo identification and at least one other non-forged/non-altered form of identification.*

A customer seeks to execute a vehicle credit sale or lease and take delivery of the vehicle off-site—at a location other than Dealership's facility. *Advise customers inquiring about off-site delivery that all paperwork, credit report, and identification procedures used by Dealership for both buyers and co-buyers apply to both on-site and off-site deliveries. Do not open the account if customer directly or indirectly seeks to avoid compliance with all identification requirements.*

A co-buyer or co-lessee is included in the vehicle credit sale or lease but is not present at Dealership facility to sign the contract or lease.
Advise customers that all paperwork, credit report, and identification procedures used by the Dealership for both buyers and co-buyers apply to all transactions. Do not open the account if customer directly or indirectly seeks to avoid compliance with all identification requirements.

PART FOUR—ADDRESS DISCREPANCY RULE

13. Policies and Procedures Following Receipt of a Notice of Address Discrepancy

In compliance with the Address Discrepancy Rule, it is the policy of Dealership not to use any consumer report for which a Notice of Address Discrepancy is received unless after following the procedures set forth below a reasonable belief can be formed that the consumer report relates to the consumer about whom Dealership requested the report.

A *Notice of Address Discrepancy* is a notice provided to the user of a consumer report by a national consumer reporting agency pursuant to a provision of the FCRA as amended by FACTA, 15 U.S.C. 1681c(h)(1). The notice informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer. When Dealership receives a Notice of Address Discrepancy, the following policies and procedures will be observed:

- The consumer report shall not be used to open an account or for any other purposes unless and until the following steps are completed:
    - Follow all Red Flag detection methods specified in Dealership's ITPP, including but not limited to the identity verification procedures, and compare the information obtained by following those methods with the information contained in the consumer report provided by the consumer reporting agency.
    - If the information from these two sources is sufficiently consistent to support a reasonable belief that the consumer report relates to the consumer about whom Dealership requested the report, the report may be used and, subject to all other provisions of this Program, the account may be opened.
    - If the information from these two sources is not sufficiently consistent to support a reasonable belief that the consumer report relates to the consumer about whom Dealership requested the report, the report may not be used and the account may not be opened. The Program Coordinator should be informed of this situation and should take any additional prevention or mitigation responses as may be appropriate under this Program.

14. Dealership to Furnish Correct Address to a Consumer Reporting Agency Following Notice of Address Discrepancy

Where required by the Address Discrepancy Rule, Dealership will report the consumer's correct address to the consumer reporting agency that issued a Notice of Address Discrepancy to Dealership.

Dealership is required to, and will, furnish the information only if all of the following conditions are met:

- Dealership regularly and in the ordinary course of business furnishes information to the credit reporting agency (primarily credit experience information).
- Dealership can form a reasonable belief that the consumer report relates to the consumer about whom Dealership

requested the report.

- Dealership establishes a continuing relationship with the consumer—that is, opens an account with the consumer.
- Dealership reasonably confirms a correct address for the consumer by one of the following means:
    - Verifying the address with the consumer about whom it has requested the report
    - Reviewing its own records to verify the address of the consumer
    - Verifying the address through third-party sources
    - Using other reasonable means

Dealership will provide the reasonably confirmed consumer address to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which Dealership establishes a relationship with the consumer—that is, the period within which the account is opened.

PART FIVE—TRAINING, SERVICE PROVIDER OVERSIGHT, AND PROGRAM UPDATING

15. Training

It is the responsibility of the Program Coordinator and Compliance Officer to ensure that all relevant Dealership personnel receive training, as necessary, to effectively implement the Program. The training will include, at a minimum, the following:

- Distribution of a copy or copies of this Program or relevant provisions taken from it to all employees having duties that may involve the opening of covered accounts or requesting or using consumer reports. Each employee shall sign a written acknowledgment of his or her understanding of and agreement to abide by the Program.
- Training of all new employees having duties that may involve the opening of covered accounts or requesting or using consumer reports.
- Training on a recurring, periodic basis, at least once each year, or as otherwise determined by the Compliance Officer to be necessary to reflect changes to the Program.

Such training program shall include, at a minimum, the pertinent requirements of the Red Flags and Address Discrepancy Rules, the policies and procedures set forth in this Program, as updated from time to time, and the importance placed by Dealership on compliance with the Program and the prevention and mitigation of identity theft.

16. Overseeing Service Providers

It is the responsibility of the Program Coordinator and Compliance Officer to exercise appropriate and effective oversight of service provider arrangements. A service provider means a person who provides a service directly to Dealership in connection with one or more covered accounts.

All service providers to Dealership performing activities in connection with covered accounts, if any, must conduct their activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Specifically, Dealership will, by contract, require its service providers that perform activities in connection with one or more of the Dealership's covered accounts to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and take appropriate steps to prevent or mitigate identity theft.

17. Reports

The Program Coordinator and other staff responsible for the development, implementation, and administration of the Program shall report to the Compliance Officer, at least annually, on compliance by Dealership with the Red Flags Rule and this Program.

The report shall address material matters

related to the Program and evaluate all material issues arising in connection with the Program since its inception or the most recent prior report. In any event, the following issues shall be addressed in each report:

- The effectiveness of the policies and procedures of Dealership in addressing the risk of identity theft in connection with the opening of covered accounts and, if and when applicable, with respect to existing covered accounts
- Service provider arrangements
- Significant incidents involving identity theft and management's response
- A summary of entries in the ID Theft Experience and Awareness Log
- Recommendations for material changes to the Program

18. Periodic Updates

It is the responsibility of the Compliance Officer to ensure that the Program is updated periodically. In addition to regular updates, the Compliance Officer may direct that a Program update or modification take place at any time, based on the existence of appropriate circumstances, such as the issuance of regulatory guidance, Dealership's experience with identity theft, or new methods of identity theft having been uncovered.

Prior to the regular periodic update, the following shall be completed as provided in this Program:

- The reporting referred to in the previous section
- An updated Risk Assessment
- An updated Identification of Covered Accounts
- An updated Identification of Relevant Red Flags
- Any necessary changes to Dealership's Red Flags detection and response procedures

All relevant information learned since the inception or prior update of the Program will be considered in performing the update, including, without limitation, the following:

- The experiences of Dealership with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that Dealership offers or maintains
- Changes in the business arrangements of Dealership, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements
- The updated Risk Assessment, Identification of Covered Accounts, and Identification of Red Flags.

Material changes to the Program must be approved by the Compliance Officer.

APPOINTMENTS AND APPROVAL

Identification of Responsible Employees

The following employees have been appointed to the positions indicated below, subject to modification from time to time as permitted under Section 3:

COMPLIANCE OFFICER

John P Byrne

PROGRAM COORDINATOR(S):

Darlene Spall

Todd Kennedy

PROGRAM APPROVAL

By signing below, the undersigned, President of Jack Byrne Ford & Mercury, acknowledge the approval of the foregoing Identity Theft Prevention Program (representing the Dealership's initial Identity Theft Prevention Program adopted pursuant to the Red Flags Rule) and the foregoing designations of the initial Compliance Officer and Program Coordinator(s).

_____

John F Byrne, President