Driven

L50

NADA MANAGEMENT SERIES

A DEALER GUIDE TO THE

FTC Red Flags and Address Discrepancy Rules:

Protecting Against Identity Theft

L50

NADA-ATD Resource Toolbox

The National Automobile Dealers Association (NADA) has prepared this management guide to assist its dealer members in being as efficient as possible in the operation of their dealerships. The presentation of this information is not intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

This guide explains a Federal Trade Commission (FTC) rule that requires automobile dealers and other creditors to develop, implement, and maintain a comprehensive written Identity Theft Prevention Program. It also addresses a separate FTC rule involving the receipt of notices of address discrepancies from a consumer reporting agency when requesting a consumer report. The guide provides a sample template to assist dealers in preparing their Identity Theft Prevention Program as well as step-by-step instructions for using the template.

Nothing in the guide is intended as legal advice. The requirements of the laws and rules covered in this guide are too complex and the circumstances of each dealership are too varied simply to adopt our model Sample Identity Theft Prevention Program without proper modifications. In addition, this guide discusses only the federal Red Flags and Address Discrepancy Rules. It does not discuss state or local law that may impose additional requirements, or other federal laws pertaining to other aspects of identity theft. It is essential that you draft a written Identity Theft Prevention Program that is appropriate to your dealership and that you have it reviewed by qualified legal counsel. Dealers must be in full compliance with the requirement to have an Identity Theft Prevention Program in place by November 1, 2008.

A DEALER GUIDE TO THE

Driven FTC Red Flags and Address Discrepancy Rules

Table of Contents

SECTION ONE

SECTION TWO

A DEALER GUIDE TO THE

FTC Red Flags and Address Discrepancy Rules

SECTION ONE

INTRODUCTION

Many automobile dealers are all too familiar with identity theft. Maybe it's happened to you:

A customer walks into the showroom, expresses interest in a vehicle, and completes a credit application to learn about financing options. You enter into a deal with the customer, who drives his new vehicle off the lot, and you send the deal over to the finance source that conditionally agreed to take assignment of the credit contract. Later, the finance source notifies you that there is a problem—the customer is not who he claimed to be. By that time, the vehicle is gone, you are on the hook for the loss, and you have only the fraudulent information the customer provided you to track him down. You quickly conclude that you have just been victimized by identity theft to the tune of tens of thousands of dollars.

While this problem remains relatively rare, it is growing, and the victims include not only the dealer but also the unsuspecting individual whose identity has been stolen. Because of these risks, and simply as a good business practice, most dealers already have extensive policies and procedures in place to confirm the identity of their customers. Many businesses and other industries, however, have not been as diligent. As a result, Congress stepped in and enacted several new requirements with which all financial institutions and creditors, including most dealers, must comply.

The Red Flags and Address Discrepancy Rules

According to the Federal Trade Commission (FTC), identity theft "occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes."[1] In an attempt to combat this growing problem, Congress directed the FTC and other federal agencies to issue several new identity theft regulations and guidelines pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[2] On November 9, 2007, the FTC and federal banking agencies fulfilled this mandate by issuing their final Red Flags Rule and Address Discrepancy Rule.[3]

The basic idea behind the Red Flags Rule is that identity theft can be reduced if businesses have policies and procedures in place to spot and prevent it. Recognizing that each business is different, the regulators determined that each business subject to the rule should create its own policies and procedures based on its specific circumstances and then set forth those policies and procedures in a formal written program, known as an **Identity Theft Prevention Program** ("ITPP" or "Program").

In short, the Red Flags Rule[4] generally requires each dealer who offers or maintains *consumer credit*, such as installment sale contracts and

vehicle leases, and *business credit* where a reasonably foreseeable risk of identity theft exists to the dealer or its customers, to do three things. These are:

1) Identify relevant Red Flags that apply to these types of credit (known as "covered accounts").
2) Develop reasonable policies and procedures to identify, detect, and respond to those relevant Red Flags.
3) Ensure that those policies and procedures are updated periodically to reflect new risks from identity theft.

Dealers must develop, adopt, and implement a written ITPP that contains these policies and procedures no later than November 1, 2008.

What is a "Red Flag"?

A *Red Flag* is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

The Address Discrepancy Rule is a separate but related identity theft prevention regulation that also has a November 1, 2008 mandatory compliance date. It requires dealers and other users of consumer credit reports to adopt policies and procedures to verify that a consumer report relates to the correct individual when the user receives a Notice of Address Discrepancy from a consumer reporting agency (CRA). Nationwide CRAs must submit this notice to a dealer who orders a consumer credit report when the consumer's address as submitted by the dealer to the CRA substantially differs from the address the CRA has on file for the consumer.

While sharing a similar goal, these new rules should not be confused with another current identity theft prevention rule, the FTC Safeguards Rule under the Gramm-Leach-Bliley (GLB) Act. This ongoing requirement, which took effect in May 2003, requires dealers and other financial institutions to develop a written program to protect customer information at the dealership from would-be identity thieves. Simply put, the Safeguards Rule seeks to prevent data maintained by the dealer from being stolen, while the Red Flags and Address Discrepancy Rules seek to prevent would-be identity thieves from using stolen data (from whatever source) to fraudulently obtain credit.[5]

Using This Guide

Section One of this guide explains the basic requirements of the Red Flags and Address Discrepancy Rules, contains answers to frequently asked questions arising under these rules, and provides a step-by-step guide to complying with the Red Flags Rule. Section Two contains a Sample ITPP and Worksheets at Attachments A and B to assist you in developing your ITPP. The appendices contain additional templates to assist you with your compliance responsibilities and include Sample Clauses to Include in Service Provider Agreements (Appendix A) and a Sample Compliance Report (Appendix B).

The Sample ITPP is designed to be a starting point from which you can develop your own written Program specific to your dealership. It is not intended to be a readymade program that you simply reproduce as your own. In fact, because each dealer's operations are different, it is unlikely that any two written Programs will be the same.

Compliance Requirements Not Covered in this Guide

Please note that this guide focuses exclusively on the federal requirements under the Red Flags and Address Discrepancy Rules. The guide does not cover the numerous other federal laws and regulations dealing with other aspects of identity theft, such as:

- The FACT Act requirements for
  - Responding to fraud alerts and active duty alerts that appear on credit reports
  - Disposal of information from consumer credit reports (also known as the FTC Disposal Rule)
  - Preventing the refurnishing of reports to CRAs after a claim of identity theft
  - Providing information to and handling the claims of victims of identity theft, including complying with prohibitions regarding the sale, transfer, and placement for collection of certain debts claimed to have resulted from identity theft
  - Debit and credit card truncation
  - Protecting medical information in the credit application process (also known as the Federal Reserve Board's Regulation FF)
- The GLB requirements contained in the FTC Privacy Rule governing the sharing and use of personally identifiable information with third parties
- The GLB requirements contained in the FTC Safeguards Rule governing the safeguarding of customer information

In addition, the guide does not cover any applicable state or local law requirements, such as state "credit freeze" laws placed on creditors by states and localities. ■

THE FTC RED FLAGS RULE

The Basics

As mentioned above, the idea behind the Red Flags Rule is to require businesses that offer credit to establish policies to detect and thwart identity thieves. The primary goal of the Red Flags Rule in the dealership context is to prevent an identity thief from financing or leasing a vehicle in someone else's name.

With that said, however, the Rule applies to much more than just automobile finance or lease transactions. It applies to all consumer finance accounts and may apply to some business accounts throughout the dealership. Indeed, the first requirement under the Rule is for dealers to review all of the different types of accounts they offer to identify those that could be subject to identity theft. After dealers have determined each account type that could be at risk of identity theft, they must then figure out what indicators of identity theft may be relevant to those types of accounts, implement procedures to detect those indicators, determine what reasonable steps the dealer should take if they are detected, and then create a Program that administers and updates these and other steps on an ongoing basis.

With all that in mind, let's take a closer look at the Rule and the guidance the FTC provides on how to comply.

Appointing a Team to Develop and Implement the ITPP

The first step that a dealer should take in complying with the Red Flags Rule is to appoint the internal personnel who will be responsible for the dealership's ITPP.

Board of Directors/Senior Management

The Rule requires the dealership's board of directors, an appropriate committee of the board, or a designated employee at the level of senior management to be involved in the Program's oversight, development, implementation, and administration. The oversight function should include assigning specific responsibility for the Program's implementation, reviewing required compliance reports by staff who are assigned implementation functions (discussed below), and approving material changes to the Program as new identity theft risks emerge.

In addition, the board of directors or an appropriate board committee must **approve** the initial written Program. If the dealership does not have a board of directors, the approval must come from a designated employee at the level of senior management.

Staff

The Rule contemplates that "staff" will be responsible for implementing the Program and drafting and presenting compliance reports to the board.

Team Approach

Thus, establishing the ITPP lends itself to a task force or team approach not only because of the multiple duties involved, but also because the Red Flags Rule envisions a division of responsibility between management and staff.

The approach followed in the Sample ITPP is to appoint a member of senior management as the "Compliance Officer" as early as possible in the process. The Compliance Officer will be responsible for the oversight, development, implementation, administration, and approval of material changes to the Program. There is no requirement to use this title, but the Rule does require a member of senior management (or the board or board committee) to fulfill this role.

To fulfill the staff roles mentioned in the Rule, the Sample ITPP calls for designation of a "Program Coordinator" (or, where necessary, a team of Program Coordinators). Again, the Rule does not require use of this title, but it does require assignment of specific responsibility for completion of these tasks. It may be advisable to name as Program Coordinator the same employee who serves as Program Coordinator under your Customer Information Safeguards Program under the FTC Safeguards Rule.

More important than the actual titles used is the timing of the appointments. The Compliance Officer and Program Coordinator(s) should be identified as early as possible to allow them to be involved in developing and drafting the Program, as well as in administering it after it is completed and approved.

Identifying "Covered Accounts"

Once the compliance personnel are in place and their duties are outlined, the first step they should take is to review all of the different types of "accounts" the dealership offers or maintains and determine whether any of them are "covered accounts." (As a threshold matter, you are only required to develop and implement an ITPP if you offer or maintain one or more "covered accounts.")

What is an Account?

The Rule defines "account" as "a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or **business** purposes." This includes "an extension of credit, such as the purchase of property or services involving a deferred payment."

This definition casts a wide net over any extensions of credit—whether for personal or business purposes. The reference to "continuing relationship," however, appears to exclude from consideration those one-time transactions that may have an element of credit risk to them, but which are not intended to continue for any length of time. For example, paying off a trade-in vehicle prior to receipt of the title certificate or accepting a personal check or credit card for parts, service, or as full payment for a vehicle all involve a degree of credit risk. However, the commentary to the Rule explains that one-time transactions such as these are not covered because "the burden that would be imposed upon financial institutions and creditors by a requirement to detect, prevent and mitigate identity theft in connection with single, non-continuing transactions by non-customers would outweigh the benefits of such a requirement."[6]

What is a Covered Account?

The Red Flags Rule does not apply to all accounts, but rather only to "covered accounts." If you offer or maintain any covered accounts, then you must implement an ITPP that applies to those covered accounts. The Red Flags Rule's definition of covered account is two-pronged and any account that falls within either prong is included. The two types of covered accounts are:

1. **Consumer Accounts.** Accounts offered or maintained for personal, family, or household purposes that involve or are designed to

permit multiple payments or transactions, such as a consumer automobile installment sale contract or lease; and

2. **Other Accounts.** Other accounts (such as commercial or business accounts) offered or maintained by the dealer for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the dealership from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The first part of this definition includes accounts where consumers make multiple payments, including consumer retail installment sales contracts and leases. Most dealers **offer** these accounts even if they do not maintain them (because they routinely assign them to a third-party finance source or leasing company). Others, such as dealers with Buy-Here, Pay-Here financing or in-house leasing companies, both **offer and maintain** consumer accounts. Dealers that engage in either type of transaction with consumers (entering into and assigning finance and lease contracts to finance sources or holding the paper themselves) will be required to develop and implement an ITPP because they offer and/or maintain covered accounts.

The second part includes "other accounts," which are not covered accounts unless there is a reasonably foreseeable risk from identity theft. These "other accounts" consist of (a) business accounts and, apparently, (b) non-multiple payment consumer accounts that still involve a continuing relationship (see **Frequently Asked Questions** for possible examples of b).

Practice Tip

You should assume that a covered account includes any and all extensions of credit—beyond a single payment transaction—offered or maintained by your dealership to consumers and, if there is a reasonably foreseeable risk of identity theft, to business customers as well.

Risk Assessment

Most of a dealer's accounts will be easily categorized as covered or not covered. However, there may be some "other" accounts offered or maintained where it is not readily apparent. Under the Rule, you must review these accounts to determine whether enough risk exists to elevate any of them to the status of a covered account. This process is referred to in the Rule as a "Risk Assessment." The Risk Assessment must take the following factors into consideration:

- The methods the dealership employs to **open** its accounts
- The methods the dealership employs to **access** its accounts
- The dealership's **previous experiences with identity theft**

The types of risk at issue in evaluating these factors are reasonably foreseeable financial, operational, compliance, reputational, or litigation risks to customers or to the safety and soundness of the dealership from identity theft.

In other words, considering the way you open or provide access to your non-consumer accounts, would an identity theft attempt against any of those accounts pose risks to your customers or to the dealership? For example, what are the chances that an identity thief could:

- Cost you or your customers money?
- Harm your reputation or that of your customers?
- Result in lawsuits against you or your customers?

Or, has the dealership experienced an incident of identity theft in relation to that account in the past?

If any of these risks are reasonably foreseeable, your Risk Assessment may conclude that the account is a covered account.

You must conduct an initial Risk Assessment prior to November 1, 2008, and periodic Risk Assessments thereafter to determine whether any of your non-consumer accounts are associated with a reasonably foreseeable risk of identity theft and thus are covered accounts that must be included in your ITPP.

The Sample ITPP in Section Two is followed by Attachment A, "Account Identification and Risk Assessment Worksheets," to assist you in identifying your covered accounts.

The Worksheets include the following account types, some of which may not be offered by your dealership:

- Consumer installment sale contracts
- Consumer vehicle leases
- Business installment sale contracts
- Business vehicle leases
- Business open accounts for parts, service, and daily rentals
- Business receivable accounts for parts and labor supplied to vehicle manufacturers under warranty and to service contract obligors
- Consumer parts or service charge accounts issued by the dealership
- Employee charge accounts issued by the dealership
- Any other extension of credit or deferred payment program, except those involving no continuing relationship

Keep in mind that any multiple-payment consumer account is considered a covered account, whereas other accounts depend on the identity theft risk posed. To the extent that your business and consumer vehicle installment sales and leases are handled in a similar manner and are open for business to the public generally, including those business accounts as covered accounts should not impose any significantly increased burden on the dealership.

Application to Commercial Truck Dealers

Medium- and heavy-duty truck dealers that engage solely in business-to-business transactions may determine that they do not offer or maintain any covered accounts and thus do not need to develop and implement an ITPP. If this determination is correct, the dealer nonetheless must conduct an initial Risk Assessment to verify that it does not offer or maintain any covered accounts, and the dealer must conduct periodic Risk Assessments thereafter to determine if any changes to the accounts it offers or maintains or new identity theft risks elevate any of its accounts to the status of a covered account (which would then require the dealer to develop and implement an ITPP). In addition, as discussed below, the dealer still must comply with the Address Discrepancy Rule if it orders consumer credit reports.

Substantive Elements of the ITPP

With all of your covered accounts identified and the scope of your Program defined, you can now assemble the Program. As discussed below, your ITPP must consist of reasonable policies and procedures to:

- **Identify** relevant patterns, practices, and specific forms of activity signaling the possible existence of identity theft (Red Flags) for each of your covered accounts
- **Detect** relevant Red Flags that you identify

- **Respond** appropriately to any relevant Red Flags that are detected to prevent and mitigate identity theft
- **Review and update** the Program periodically to reflect changes in risks from identity theft

Identifying Relevant Red Flags

In determining which Red Flags are relevant to each of your covered accounts, you must consider the following areas:

- Risk factors
- Categories of Red Flags
- Other sources of Red Flags

Risk factors

The risk factors for purposes of identifying relevant Red Flags are the same as those used in your Risk Assessment to identify your covered accounts (i.e., for each covered account, you must analyze the methods the dealership employs to open and access the account and the dealership's previous experiences with identity theft).

Because of the overlap between the Risk Assessment involved in identifying covered accounts and the risk factors analysis required to determine relevant Red Flags for each covered account, the previously mentioned Account Identification and Risk Assessment Worksheets are designed to be used for both purposes.

Categories of Red Flags

The second area you must consider are the following categories of Red Flags:

- Alerts, notifications, or other warnings received from CRAs 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 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 your covered accounts

The FTC sets forth 26 illustrative examples of Red Flags ("Example Red Flags") from these categories, which you should analyze and, if you determine them to be relevant, incorporate into your ITPP. The "Red Flag Identification, Detection, and Response Worksheets" (Attachment B) to the Sample ITPP in Section Two lists each Example Red Flag.[7]

When analyzing the relevance of the 26 Example Red Flags, keep in mind that this list was developed jointly by the FTC and the federal banking regulatory agencies with all financial institutions and creditors in mind, not just dealers. Therefore, while many are likely to be relevant to your covered accounts, others are not likely to be relevant.

For example, certain Example Red Flags, such as Number 5 ("documents provided for identification appear to have been altered or forged") and Number 6 ("the photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification"), would appear highly relevant to most dealers' covered accounts (and, in these instances, are likely already part of your existing policies and procedures to prevent identity theft). In contrast, others, such as Number 20 that pertains to revolving credit accounts, clearly are not relevant to dealers that do not offer such accounts.

The larger challenge exists with Example Red Flags that appear to provide useful information but perhaps are not reasonable to adopt in light of their cost, burden, and the fact that you currently possess or will adopt other customer identification procedures that diminish their relevance.

For example, Number 10b ("the Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File") mentions useful information. However, as noted in the "General Guidance on Identifying Relevant Red Flags" (see below), the FTC is not expected to suggest that a Red Flag is "relevant" (and therefore required to be included in the ITPP) simply because it could theoretically be helpful in preventing identity theft. The FTC might ask, however, whether the Red Flag would realistically increase your chances of detecting and preventing identity theft. With respect to Number 10b, the answer to that question would be "no" if you determine from your Risk Assessment that it is highly unlikely that an identity thief could use a deceased person's or non-issued SSN to circumvent your customer identification procedures and your other Red Flag detection methods. Keep in mind, however, that circumstances can change and that if implementation of Number 10b (or any other Red Flag) should become less expensive or less difficult for whatever reason, your relevance determination may change. You should review your assessments when you review and update your program.

Other Sources of Red Flags

The third area you must consider are other sources of Red Flags, including:

- Incidents involving identity theft the dealership has experienced
- Methods of identity theft the dealership has identified that reflect changes in identity theft risks
- Applicable supervisory (FTC) guidance

Another source of Red Flags may come from the dealership's existing policies and procedures for preventing identity theft.

These requirements recognize that past identity theft incidents at the dealership are clear indicators of the threat of identity theft in the future, and that the tactics used by identity thieves are constantly evolving. The dealership must account for these changing tactics when developing and updating its ITPP. Because the list of relevant Red Flags must be updated periodically, the dealership should adopt a procedure that will include in the Program update any information the dealership maintains concerning identity theft incidents and changed methods

General Guidance on Identifying Relevant Red Flags

In determining what Red Flags are relevant to your covered accounts and thus must be incorporated into your ITPP, keep in mind:

- Even with the Rule's directives regarding risk factors and categories and sources of Red Flags, there is very little guidance in the Rule concerning exactly how to create a set of "relevant" Red Flags for incorporation into your ITPP.
- The lack of definitive and bright-line rules is acknowledged by the regulators, who refer to the Rule's Red Flag identification provisions as taking "a risk-based, non-prescriptive approach."
- The FTC is not expected to suggest that a Red Flag is "relevant" simply because it could theoretically be helpful in preventing identity theft.
- The Red Flags Rule calls for the dealership to adopt *reasonable* policies and procedures for the identification of relevant Red Flags. Although you should take a cautious approach toward your regulatory obligations, there is no prohibition against considering factors such as feasibility and cost when developing your ITPP policies and procedures.

of identity theft. The Sample ITPP suggests that the Program Coordinator develop a log of dealership identity theft incidents for this purpose.

In the end, the Example Red Flags and other potential Red Flags identified by your dealership should be evaluated in light of the risk factors for covered accounts; the categories and sources of Red Flags; the dealership's size, complexity, and the nature and scope of its activities; the dealership's existing identity theft prevention policies; the cost and availability of establishing methods to detect a particular Red Flag; and whether, in light of these considerations and other relevant facts, it would be reasonable and appropriate for you to identify the Red Flag as relevant and include it in your ITPP.

Developing the Means to Detect Red Flags and Verify Identity

Once you have identified Red Flags that are relevant for each type of your covered accounts, the next step under the Rule is to develop reasonable policies and procedures to detect those relevant Red Flags by appropriate means, such as:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account
- Where the dealership maintains a covered account after it is opened, authenticating customers, monitoring transactions, and verifying the validity of change of address requests

The Red Flags and Address Discrepancy Rules each identify the Customer Information Program (CIP) rules under section 326 of the USA PATRIOT Act (also known as the "Know Your Customer" rules) as a means of verifying a customer's identity.[8] The CIP rules require (and to a great extent provide) reasonable procedures for verifying the identity of any person seeking to open an account; maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to financial institutions by the government.

Dealers presently are not required to adopt the identity verification procedures contained in the CIP rules.[9] Nonetheless, should dealers choose to adopt and implement them, they would serve as a permissible Red Flag detection method under the Red Flags Rule and also, as discussed below, one of several means of satisfying your customer identification responsibilities under the Address Discrepancy Rule.

If you choose not to adopt the CIP procedures, you must develop other identity verification procedures for persons opening an account. **For purposes of complying with the detection component of the Red Flags Rule, consider applying the procedures you develop to respond to Notices of Address Discrepancy to any situation involving the opening of a covered account, even those not involving the receipt of a Notice of Address Discrepancy from a CRA.** Although the procedures may vary depending on the type of account involved, identity verification should become (if it is not already) a standard operating procedure for your dealership to use for any person seeking to conduct business with your dealership.

Beyond identity verification, you also should consider additional means that may be useful in detecting each of the relevant Red Flags that you have identified. The approach suggested in the Sample ITPP is to use the Red Flag Identification, Detection, and Response Worksheets for this purpose. The Worksheets provide space to set forth specific detection methods for each relevant Red Flag. After you complete the process for all relevant Red Flags, the detection methods can be collected and edited, and you can develop a list of customized detection methods. This list, along with the identity verification procedures you adopt, should allow you to establish an effective detection mechanism for the relevant Red Flags you have identified.

Examples of Detection Methods

The detection method describes exactly what steps dealer personnel need to take to detect a relevant Red Flag. Again, Red Flags that are extremely difficult or impossible to detect are not likely to be deemed "relevant," so to an extent, the detection determination is closely connected to the identification of relevant Red Flags. In the end, it should include any reasonable method available to the dealer to detect a relevant indicator of identity theft.

For example, some detection methods include:

- Closely inspecting documents provided for identification
- Comparing the information provided by the consumer with other information the dealership has on file about that consumer
- Reviewing the consumer credit report for such things as fraud alerts, active duty alerts, or notices of address discrepancy
- Reviewing the credit report for unusual patterns or activity
- Asking verification questions based on information contained in the credit report
- Listening carefully for suspicious statements by the credit applicant
- Comparing signatures

Of course, not all detection methods make sense for all Red Flags. A review of the Red Flag Identification, Detection, and Response Worksheets provides numerous examples. Dealership personnel with experience in confirming identity and/or requesting and reviewing credit reports should be consulted when developing the detection methods. You should keep track of which detection methods are effective and which are ineffective, and update your ITPP accordingly.

Developing Policies and Procedures for Responding to Detected Red Flags

The Rule also requires the ITPP to include reasonable policies and procedures to respond appropriately to detected Red Flags to prevent and mitigate identity theft. The responses are to be commensurate with the degree of risk posed, considering aggravating factors.

The approach suggested in the Sample ITPP is to list the response approach you will follow for each relevant Red Flag you detect on the Red Flag Identification, Detection, and Response Worksheets.

Again, the responses will depend in large part on the nature and severity of the Red Flag detected, and should take into account the quality and quantity of the Red Flags present in any one transaction. Further, your approach should provide for a range of responses based on the circumstances and the judgment of the personnel involved. Because not every response is appropriate in every circumstance, the Sample ITPP takes a three-pronged approach to response policies and procedures.

First, to give the dealership maximum flexibility, the Sample ITPP establishes General Response Procedures that permit a range of possible responses, based on the facts and circumstances that exist when a Red Flag is detected.

Second, the General Response Procedures recognize that there are many detected Red Flags that can be cleared through a reasonable investigation.

Consequently, it establishes a procedure where the employee who detects the Red Flag works with his or her manager to assess the level of risk present. If they cannot negate their suspicion of identity theft, they will not open the account and the matter will be referred to the Program Coordinator for any further response. If, on the other hand, the investigation removes their suspicion of identity theft, they will proceed with opening the account.

Third, the Sample ITPP recognizes that the detection of some Red Flags requires the dealership to take specific actions, such as following the procedures to respond to a fraud or active duty alert (which is a separate duty under section 112 of the FACT Act and also is set forth by the FTC as Example Red Flag Number 1) or to a Notice of Address Discrepancy (which, as discussed below, is a separate duty under section 315 of the FACT Act and also is set forth by the FTC as Example Red Flag Number 3). The Sample ITPP contains sample Specific Response Procedures, intended to supplement the General Response Procedures, for these and other situations.

Developing Policies and Procedures to Update the ITPP

Once you have established your procedures for identifying, detecting, and responding to relevant Red Flags, you must develop policies and procedures to update your ITPP periodically.

The Red Flags Rule directs that updates appropriately reflect changes in risks, based on factors such as:

- The experiences of the dealer 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 the dealership offers or maintains
- Changes in the business arrangements of the dealership, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements

In light of the Rule's requirement for an annual compliance report (discussed below), it should be reasonable to perform your Program update annually after the compliance report has been reviewed and considered. As part of the updating process, you should review the identification of covered accounts and relevant Red Flags and reassess the effectiveness of your current detection and response procedures. You also should address necessary changes to the administrative elements of your ITPP (see discussion below).

In addition, should you encounter a significant change in circumstances, such as a serious incident of identity theft or installation of a new credit report retrieval system, you should immediately update the Program (at least to the extent relevant to the changed circumstance).

Administrative Elements of the ITPP

After the written Program has been developed in accordance with the guidelines above, the Red Flags Rule sets forth certain steps that dealers must take to administer it.

Training

The ITPP should include policies for training all relevant dealership personnel. Relevant personnel include those who perform functions covered by the ITPP, including employees involved in opening covered accounts, working with existing accounts (if any), or, as required by the Address Discrepancy Rule, requesting or using credit reports.

See the Sample ITPP in Section Two for sample policies and procedures applicable to training.

Overseeing Service Providers

The Rule also requires dealers to "oversee service provider arrangements effectively and appropriately."

When engaging a service provider to perform an activity in connection with one or more covered accounts, the dealer should ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. As an example, the Rule notes that the service provider could be asked to sign a contract requiring the service provider to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the dealer or take appropriate steps to prevent or mitigate identity theft. Appendix A contains sample clauses that may be appropriate to include in your contracts with your service providers.

Under the Rule, a service provider means a person who provides a service directly to the dealership in connection with one or more covered accounts. This is an extremely broad definition.

Despite the breadth of the definition and of the triggering event that requires service provider oversight (engaging a service provider to perform "an activity" in connection with covered accounts), it appears the regulators are concerned here with a set of circumstances that may be somewhat infrequent among automobile dealers.

The intent of this requirement is twofold: to make it clear that a creditor or financial institution cannot escape duties under the Red Flags Rule simply by delegating or outsourcing them to outside entities, and to ensure that any entity performing such duties observes the requirements of the Rule. Therefore, there would be no point in including an entity within the "service provider" definition unless the activities it performs are, at least in part, activities implicated by the Rule, such as opening covered accounts or having some responsibility for servicing or maintaining covered accounts in a manner involving a relevant Red Flag.

Dealers whose covered accounts are limited to installment sale contracts and leases and who immediately assign those agreements to finance sources do not maintain or service covered accounts, and thus do not retain service providers to maintain or service those accounts. And, with respect to opening such accounts, most of those dealers do not outsource the actual account opening functions.

However, the following arrangements may be examples of the use of service providers in the opening of covered accounts:

- A broker or other third party acting on behalf of the dealer secures the customer's signature on installment sale contracts or leases.
- A vendor of identity theft prevention services retained by the dealer performs the duties of the dealer under the Red Flags Rule with respect to each potential covered account.

On the other hand, a vendor that creates and hosts dealer websites—even those that contain an online credit application—would not appear to be a service provider who would be required to detect relevant Red Flags unless that vendor is actually engaged by the dealer to make some use of the information obtained through the website (such as information contained in the online credit application) as part of the process of opening the account. For example, the vendor may be a service provider subject to the regulations if the dealer engages the vendor to review the credit application or other information supplied by the consumer for certain information that would otherwise be reviewed internally at the dealership as part of the account opening process.

Dealers who hold covered accounts for a period of time after they are opened may engage service providers to perform activities on the accounts that would trigger the service provider requirement. For example, outsourced customer service centers or other agents serving as the customer's principal

point of contact on the account would likely be considered "service providers" under the Rule.

In the event your dealership outsources to or relies on service providers as part of the account opening or maintenance process, you should exercise appropriate and effective oversight of them. This includes carefully selecting the vendor and, as contemplated by the Rule, obtaining a contractual commitment that the service provider will have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the dealer or take appropriate steps to prevent or mitigate identity theft.

Board Approval of the ITPP

Once the ITPP has been drafted, the Rule requires that it be approved by the dealer's board of directors or an appropriate board committee. For dealers that do not have a board of directors, the Rule requires approval by a "designated employee at the level of senior management."

Management Oversight

The Rule requires that the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management also perform the functions listed below:

Assigning specific responsibility for implementation of the ITPP

This is addressed above under "Appointing a Team to Develop and Implement the ITPP."

Reviewing compliance reports

The board, board committee, or senior management employee must also review the staff compliance reports (see below under "Reporting").

Approving material changes to the ITPP as necessary to address changing identity theft risks

The board, board committee, or senior management employee is responsible for approving changes to the Program either at the time of the periodic update or when required by the circumstances (for example, following an incidence of identity theft at your dealership).

Reporting

The Rule also requires that staff who are responsible for developing, implementing, and administering the ITPP report to the board of directors, board committee, or senior management employee at least annually on the dealership's compliance with the Red Flags Rule.

The report, which should be in writing, must address material matters related to the Program and evaluate issues such as:

- The effectiveness of the policies and procedures of the dealership in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts
- Service provider arrangements
- Significant incidents involving identity theft and management's response
- Recommendations for material changes to the Program

Appendix B contains a Compliance Report template to assist you with this obligation. ■

THE FTC ADDRESS DISCREPANCY RULE

Duty to Implement Policies and Procedures to Confirm Identity upon Receipt of Notice from CRA

As mentioned above, the FACT Act also requires nationwide CRAs to inform users of consumer credit reports when a substantial difference exists between the consumer address the user provided when requesting a credit report and the address(es) the CRA has on file for the consumer. Determining whether such a notice should be issued to the dealer is entirely up to the CRA.

The Address Discrepancy Rule requires a dealer to develop and implement reasonable policies and procedures to be followed when it receives a Notice of Address Discrepancy from a CRA. These policies and procedures must enable the dealer to form a reasonable belief that a credit report relates to the consumer about whom it has requested the report or determine that it cannot do so.

The Rule applies only with respect to consumer credit reports—that is, credit reports respecting an individual. (This includes consumer credit reports obtained for hiring or other employment purposes as well those obtained for vehicle financing purposes.) The Rule has no application with respect to business credit reports, unless they include a consumer credit report on the business owner.

What is a Reasonable Policy to Confirm Identity?

The Address Discrepancy Rule provides the following examples of reasonable policies and procedures a dealer could implement to confirm the applicant's identity:

1. Comparing the information in the consumer credit report with:
   - A. Information the dealer obtains to verify the consumer's identity in accordance with the CIP rules;
   - B. Information the dealer maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
   - C. Information the dealer obtains from third-party sources; or
2. Verifying the information in the credit report with the consumer.

As mentioned above, the CIP rules are a series of policies and procedures regarding customer identification and verification set forth in a separate federal statute known as the USA PATRIOT Act. Although dealers presently are not subject to the CIP rules, you may, if you have or intend to put CIP procedures in place, use those procedures as one means of verifying that you obtained the correct credit report.

If you do not have CIP procedures in place, several reasonable alternatives exist. Item 1B above, for example, allows dealer personnel to compare the credit report against information the dealer maintains in its own records, such as the credit application, driver's license, and other data gathered as part of the dealer's ITPP. Item 2 allows dealer personnel to verify or "test" the consumer on information contained in the consumer credit report. In other words, dealership personnel can verify the customer's identity by asking the customer questions about the information in the credit report, such as former addresses, amounts on credit lines, names of creditors, etc.

Whatever policies the dealer adopts, the credit report should not be used and the account opening process should not proceed unless and until dealer personnel have followed the procedures and have formed a reasonable belief that the credit report relates to the correct customer. If such a belief is formed, the report may be used and, subject to any other requirements of the ITPP (detailed below), the account may be opened. If such a belief cannot be formed—because there is still suspicion—the account should not be opened and any further responses provided for in the ITPP should be followed.

Policies to Furnish Address to Consumer Reporting Agency

Although unlikely to apply to many dealers, there is a second component of the Address Discrepancy Rule that requires certain users of credit reports to report back an accurate address for a consumer to the CRA from which it received a Notice of Address Discrepancy.

This second component applies only to dealers who regularly and in the ordinary course of business furnish information to the CRA that issued the Notice of Address Discrepancy. If you are a furnisher of information to the CRA, you must develop and implement policies and procedures to furnish the address you have for the consumer to the CRA when all the following conditions are met:

- You form a reasonable belief that the credit report relates to the consumer about whom you requested the report.
- You establish a continuing relationship with the consumer—that is, you sell on credit or lease a vehicle to the consumer or otherwise open an account.
- You reasonably confirm that the address is accurate.

Examples of reasonable confirmation methods set forth in the Rule are:

- Verifying the address with the consumer about whom you have requested the report;
- Reviewing your records to verify the address of the consumer;
- Verifying the address through third-party sources; or
- Using other reasonable means

Your policies and procedures must provide that you will furnish the address that you have reasonably confirmed is accurate to the CRA as part of the information you regularly furnish for the reporting period in which you establish a relationship with the consumer (in other words, the period in which you sell a vehicle on credit, enter into a lease transaction, or otherwise open an account). ■

Application to Commercial Truck Dealers

Medium- and heavy-duty truck dealers that obtain consumer credit reports must comply with the Address Discrepancy Rule even if they determine that they are not required to develop and implement an ITPP under the Red Flags Rule (which dealers may only determine after conducting a mandatory Risk Assessment concerning the accounts they offer).

FREQUENTLY ASKED QUESTIONS

1. What dealers are subject to the Red Flags Rule?

The Rule casts an extremely wide net that brings within its coverage a very large share of the nation's business economy. Not only are financial institutions subject to the Rule, but so are creditors. In that sense, virtually all dealers are covered by the Red Flags Rule because virtually all dealers are creditors. In fact, the Red Flags Rule specifically identifies automobile dealers in its list of creditors. However, the requirement to develop and implement an ITPP only applies to financial institutions or creditors that open or maintain "covered accounts." As discussed under "Identifying Covered Accounts," this includes multiple-payment transactions with consumers, such as retail installment sale contracts and lease agreements (even if they are immediately assigned to a third-party finance source), and also includes other accounts where there is a reasonably foreseeable risk to customers or to the dealership from identity theft. If you are a medium- and/or heavy-duty truck dealer, see the information under "Application to Commercial Truck Dealers" on page 7.

2. What dealers are subject to the Address Discrepancy Rule?

The rule applies to dealers who order consumer credit reports from a CRA.

3. Does each dealership in a dealer group need to comply individually?

Each legal entity subject to the Red Flags Rule must comply, whether or not it is owned by a dealer group that owns other dealerships. However, nothing in the Rule prohibits the dealer group from developing an ITPP for use by its individual dealer entities, provided that any unique circumstances relevant to the development and operation of the Program at the dealer-entity level is accounted for and provided that the board of directors (or appropriate board committee or, if there is no board, a designated senior management employee) for each dealer-entity approves the Program for use by that entity.

4. Am I required to have a written Address Discrepancy policy?

There is no express requirement to have a written policy to comply with the Address Discrepancy Rule. However, you must have policies and procedures to verify the identity of customers for whom you receive a Notice of Address Discrepancy, and it would be prudent to set forth those procedures in writing. The Sample ITPP contains procedures at Section 13 for this purpose.

5. Can we combine our ITPP with our Customer Information Safeguards Program under the FTC Safeguards Rule?

Yes, and doing so may have the benefit of encouraging comprehensive training for both

your safeguarding policies and your identity theft detection policies. However, the complexity of both Rules could hamper any effort to compose a unified program that complies with both Rules. In addition, although there are similarities between the Rules, they have significant differences, such as being the products of entirely separate legislative enactments with different sets of defined terms.

6. If we fall victim to identity theft, have we automatically violated the Red Flags Rule?

No. The Rule does not impose strict liability for failing to detect identity theft in any particular instance. Instead, the FTC would, upon investigation, examine the particular circumstances surrounding the incident. The focus of the Rule is on having financial institutions and creditors create and follow reasonable policies and procedures designed to prevent and mitigate identity theft, but it does not require perfect policies that eliminate the possibility of identity theft from ever occurring (hence the need to develop reasonable policies and procedures under the Rule). If the dealership does fall victim to identity theft, the Rule would require you to take everything learned from that experience into consideration in revising and updating your Program.

7. What are the penalties for violating the Red Flags or Address Discrepancy Rules?

There is no federal private right of action for violating either the Red Flags Rule or the Address Discrepancy Rule. Enforcement falls to the FTC as the agency responsible for interpreting and enforcing the Rules as they pertain to dealers. All enforcement matters begin with an investigation. When the facts point to law violations, these investigations can lead to administrative settlements. These settlements can include both injunctions that require the company to comply with the Rule, other reporting obligations, and civil penalties of up to $2,500 for each "knowing" violation of the Rule(s). If the dealer fails to comply with that order, the FTC could file a federal lawsuit seeking fines of up to $11,000 for each future violation, injunctive relief, and/or a long-term consent decree. Keep in mind that the civil penalties (up to $2,500) that may be required to resolve the investigation could apply to past violations, while fines stemming from a lawsuit apply only to future violations. If the parties do not reach a settlement, the FTC can bring an action in Federal district court for civil penalties and injunctive relief.

In addition, it is also possible that violations of these Rules could subject a dealer to state law claims (including class action claims) under state "unfair and deceptive acts and practices" (UDAP) statutes. These laws typically permit actual and punitive damages, as well as attorneys' fees and costs.

8. What are some examples of non-multiple payment consumer accounts involving a continuing relationship that may be considered covered accounts under the Red Flags Rule?

While the Red Flags Rule provides no definitive answer, one example might be a zero-down installment contract that calls for only one payment—a balloon payment—at the end of the contract term. In such an extension of credit, the continuing relationship could be seen to result from the contractual terms unrelated to payment that the buyer must observe over the duration of the contract, such as maintaining the vehicle, keeping it insured, and renewing registration. Another possible example would be a rental car contract for an extended term where only one payment is due at the end of the term even though the renter is obligated to various contractual duties during the term.

9. Under what circumstances, if any, do we need to notify law enforcement under the Red Flags Rule?

The Rule does not directly identify any circumstances that require you to notify law enforcement. The Rule includes notification of law enforcement as a possible response if such a response would prevent or mitigate identity theft considering the degree of risk posed by the Red Flag(s) you detect

and any aggravating factors. For example, if an identity thief presents identification documents that you determine are clearly counterfeit and your review of the consumer credit report reveals overwhelming evidence of ongoing identity theft, in addition to not opening the account, your Program Coordinator may determine it appropriate in accordance with state and local law to notify law enforcement. Another example where notifying law enforcement may be appropriate would be if the dealership finds that it has been targeted by a ring of identity thieves in the dealer's community that law enforcement has been attempting to apprehend.

10. Do these Rules mean that we cannot conduct transactions with persons who never come to the dealership, such as someone in another state who contacts us by phone after visiting our website?

No. The Rules do not in any way prohibit telephone, online, or interstate transactions. However, a dealer that enters into installment sale contracts or leases with customers who never come to the dealership or meet dealership employees in person will require an ITPP that takes that method of opening an account into consideration in identifying, detecting, and responding to relevant Red Flags. For example, for accounts opened remotely and without meeting the customer in person, the dealer may determine that additional Red Flags and/or customer identification methods are necessary due to the inability to physically inspect identification documents and determine, for example, if the customer's appearance matches the photograph on the identification documents. As noted in our discussion of "Substantive Elements of the ITPP," the CIP rules contain examples of "non-documentary" identity verification procedures that allow verification of identity without reliance on identification cards and other documents.

11. What documents should we retain to demonstrate compliance with these Rules and how long should we retain them?

You should retain all of the following:

- The initial and all subsequent versions and updates of your ITPP
- All documents used in the process of creating and updating your ITPP, such as worksheets and annual compliance reports
- All documents supporting your Program administration responsibilities, such as training outlines, training attendance sheets, and documents related to your oversight of service providers

These documents may be necessary if you are ever called upon to verify that you followed the required processes to develop and update your ITPP.

These documents should be retained indefinitely, or at least for the full statute of limitations (SOL) period under the laws mentioned above. Regarding the FCRA and the FTC Act, the FCRA has the longer SOL, which can extend up to five years from the date of a FCRA violation. Your state UDAP statute may impose a longer SOL period. ■

FTC RED FLAGS RULE COMPLIANCE CHART:

This chart may assist you in developing and implementing a written ITPP by the final date for complying with the Red Flags Rule (November 1, 2008). The chart highlights the general compliance steps you must take with cross-references to the Sample ITPP and the narrative portion of the guide.

STEP 1 — Appoint an ITPP Compliance Officer and an ITPP Program Coordinator.

Appoint a senior manager to serve as the ITPP Compliance Officer who will be responsible for the Program's oversight, development, implementation, and administration. If necessary, appoint an ITPP Program Coordinator to manage and coordinate the Program under the supervision of the Compliance Officer.

See Section 3 and the final page of Sample ITPP (entitled "Appointments and Approval") and narrative discussion at pp. 4 - 5.

STEP 2 — Determine the "covered accounts" that you offer or maintain.

Identify all of the "accounts" that you offer or maintain and determine which ones are "covered accounts" that must be addressed in your ITPP. Covered accounts generally consist of (1) all of your consumer transactions involving multiple payments (even if you immediately assign the contract to a third party) and (2) your other multiple payment accounts (including business accounts) where there is a reasonably foreseeable risk of identity theft to your dealership or your customers.

See Sections 4-6 and 9 of Sample ITPP and narrative discussion at pp. 5 - 7.

Use Account Identification and Risk Assessment Worksheets.

STEP 3 — Identify relevant indicators of possible identity theft ("Red Flags") for each covered account.

For each of the covered accounts you identified, determine what patterns, practices, or activities may indicate a possible attempt at identity theft. Keep in mind that "relevant" Red Flags are reasonable (as opposed to theoretical) indicators of ID theft. You must consider several sources of Red Flags, such as vulnerabilities in how you open and maintain your covered accounts, your prior experiences with identity theft (consider also methods of identity theft at other dealerships that you have learned about), and guidance from the FTC, including its list of 26 Example Red Flags.

The Worksheets to the Sample ITPP set forth the 26 Example Red Flags and other Red Flags that may apply to your covered accounts. Determine which of these, and other Red Flags that are not set forth in the Worksheets, are relevant to your covered accounts, and list them in your ITPP.

See Sections 7 and 10 of Sample ITPP and narrative discussion at pp. 7 - 10.

Use Red Flag Identification, Detection, and Response Worksheets.

STEP 4 — Develop procedures for detecting those Red Flags.

For each relevant Red Flag that you have identified, determine what reasonable methods dealership personnel must follow to detect that Red Flag. Include procedures to verify the identity of a customer who wishes to open or access a covered account, ***and*** additional detection procedures for certain Red Flags that you identify.

See Sections 8 and 11 of Sample ITPP and narrative discussion at pp. 10 - 11.

Use Red Flag Identification, Detection, and Response Worksheets.

STEP 5 — Develop procedures for responding to relevant Red Flags that you detect.

For each relevant Red Flag that you identify and detect, determine what reasonable response procedures dealership personnel must follow. The procedures should be flexible and should provide for a range of possible responses depending on the Red Flag detected and the specific facts and circumstances involved. The Sample ITPP sets forth "General Response Procedures" to be followed when any Red Flag is detected as well as additional "Specific Response Procedures" to be followed when certain Red Flags are detected.

See Section 12 of Sample ITPP and narrative discussion at pp. 11- 12

Use Red Flag Identification, Detection, and Response Worksheets.

STEP BY STEP

STEP 6 Train your employees.

Your ITPP should include policies for training all dealership personnel involved in opening or maintaining covered accounts or performing any duty set forth in your Program, including your procedures for complying with the Address Discrepancy Rule.

See Sections 13, 14 (if applicable), and 15 of Sample ITPP and narrative discussion at page 12.

STEP 7 Oversee your service providers.

If you outsource to a service provider any activity necessary for opening or maintaining covered accounts, or any duty under your ITPP (e.g., functions related to identifying, detecting, or responding to relevant Red Flags that exist with your covered accounts), ensure that your service provider has appropriate policies and procedures in place to perform these functions and agrees to do so contractually.

Note that the Sample ITPP assumes the dealership does *not* retain service providers for this purpose. If you retain service providers to which you have outsourced ITPP duties, ensure that your ITPP reflects that arrangement.

See Section 16 of Sample ITPP, narrative discussion at pp. 13 - 14, and Appendix A entitled "Sample Clauses to Include in Service Provider Agreements."

STEP 8 Draft an ITPP that details the procedures set forth above.

Consolidate the information gathered and produced to comply with each of these steps, including the information from the Sample ITPP Worksheets, and incorporate it into a formal written Program. Ensure that your ITPP is comprehensive and includes the procedures you will adopt to comply with the Address Discrepancy Rule. In addition, ensure that you document all of your compliance efforts.

STEP 9 Ensure that your board of directors or a committee of the board approves your ITPP by November 1, 2008.

Once your ITPP is drafted, it must be approved by the dealership's board of directors or an appropriate board committee by November 1, 2008. If your dealership does not have a board of directors, the ITPP must be approved by a designated senior management employee.

See Sections 1 and 3 and the "Appointments and Approval" page of Sample ITPP and narrative discussion at page 14.

STEP 10 Comply with the ongoing Program requirements.

Your compliance duties under the Red Flags Rule do not end on November 1, 2008. The Program must be continuously administered and you must adhere to a series of ongoing administrative requirements designed to ensure that your ITPP is responsive to the latest trends in identity theft.

The Program Coordinator (or staff responsible for administration of the ITPP) must submit compliance reports at least annually as detailed in the ITPP, while the Compliance Officer (or the board of directors, a board committee, or a designated senior management employee) must ensure the ITPP is updated periodically. The dealership should update its list of covered accounts, relevant Red Flags, and detection and response procedures as part of this process or sooner if warranted by the circumstances (such as if an identity theft incident occurs). The dealership also must stay current with its training obligations and service provider oversight responsibilities.

See Sections 17 and 18 of Sample ITPP, narrative discussion at page 14, and Appendix B entitled "Sample Compliance Report."

This chart is offered for informational purposes only and is not intended as legal advice. Consult your legal counsel concerning the full range of your Red Flags Rule compliance responsibilities.

ENDNOTES

[1] FTC publication, "Fighting Back Against Identity Theft," at http://ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[2] 15 U.S.C. §§ 1681 *et seq*.

[3] 72 Fed. Reg. 63,718 – 63,775 (Nov. 9, 2007). The FTC Red Flags and Address Discrepancy Rules are set forth at 16 C.F.R. Part 681. These Rules implement sections 114 and 315 of the FACT Act of 2003, respectively.

[4] The Red Flags Rule includes an Appendix containing "Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation," which "are intended to assist financial institutions and creditors" in formulating and maintaining an Identity Theft Prevention Program, and reflect the agencies' recommendations for doing so. Section 681.2(f) of the Rule states any entity that is required to implement an identity theft prevention program must consider the guidelines and include in its Program those guidelines that are appropriate. Therefore, this guide does not distinguish between the Red Flags Rule itself and these guidelines found at Appendix A to 16 C.F.R. part 681.

[5] For an overview of dealers' responsibilities under the FTC Safeguards Rule, see the NADA publication, *A Dealer Guide to Safeguarding Customer Information* (2003). See also the FTC publication, "Financial Institutions and Customer Information: Complying with the Safeguards Rule," (2006) at www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf.

[6] 72 Fed. Reg. at 63,721.

[7] The Example Red Flags are also set forth at Supplement A to Appendix A of the FTC Red Flags Rule, which is available on page 58 of the Final Rule (identified at the top of the page as 63,774) at www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf.

[8] 31 U.S.C. § 5318(l); 31 C.F.R. Part 103, Subpart I.

[9] See 31 C.F.R. 103.170 (as to section 352).

Sample Identity Theft Prevention Program (ITPP)

Note: This Sample Identity Theft Prevention Program (ITPP) is for informational purposes only. It may not be suitable for your particular dealership or operations. You are obligated to develop, draft, and implement an ITPP appropriate to your dealership and the covered accounts it offers or maintains. Ensure the Program you develop is reviewed by legal counsel familiar with applicable federal law and state and local laws that may bear on the subject of identity theft.

PART ONE—BACKGROUND

1. Effective Date

All affected employees of _____ ("Dealership") must comply with the terms of this policy as instructed by their respective supervisors but no later than November 1, 2008.

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

This sample policy was drafted with the assumption that the Dealership immediately assigns all installment contracts and leases and does not hold these or other accounts. Buy-Here, Pay-Here dealerships and other dealerships that hold covered accounts need to ensure their Program properly addresses these duties as they relate to the maintenance of existing accounts.

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 RESPONSE

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:

[List types of covered accounts for <u>your</u> dealership as reflected on the attached Account Identification and Risk Assessment Worksheets].

[The following sample list is for illustration only and may not correctly reflect the covered accounts your dealership offers:

- *Consumer vehicle installment sale contracts*
- *Consumer vehicle leases*
- *Business vehicle installment sale contracts*
- *Business vehicle leases]*

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:

[List relevant Red Flags for <u>your</u> dealership that you listed on the Red Flag Identification, Detection, and Response Worksheets.]

[Apart from the first item—which federal law identifies as a relevant Red Flag—the following sample list is for illustration only and may not correctly reflect the Red Flags that are relevant for your dealership:

- *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.*

See Red Flag Identification, Detection, and Response Worksheets for additional potential Red Flags.]

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:

[List reasonable procedures that will detect relevant Red Flags here including identity verification procedure used for <u>your</u> dealership and the detection methods you listed on the Red Flag Identification, Detection, and Response Worksheets.]

[The following sample list is for illustration only and may not correctly reflect the identity verification and Red Flag detection methods appropriate for your dealership. These detection methods include basic identity verification procedures. Your dealership's procedures may be more comprehensive due to, for example, requirements of state or local law, identity theft protection systems available to you, or your existing verification policies:

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:

[List here specific response procedures that will be used for specific Red Flags that are detected at <u>your</u> dealership. Incorporate the specific response procedures listed on the Red Flag Identification, Detection, and Response Worksheets.]

[Apart from the first two items—which reflect required responses under federal law—the following sample list is for illustration only and may not correctly reflect the specific response procedures appropriate for <u>your</u> dealership:

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:*

> Several states have specific requirements for responding to these or state-law versions of fraud alerts or credit freezes. This section would need to be revised to include those requirements, if applicable.

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. *[As of the current version of this Program, Dealership does not use service providers to perform activities in connection with covered accounts.]*

17. Reports

The Program Coordinator and other staff responsible for the development, implementation, and administration of the Program shall report to

the Compliance Officer *[or board of directors, a board committee, or other member of senior management]*, 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 *[or board of directors, committee of the board, or other member of senior management]*.

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: _____

PROGRAM COORDINATOR(S): _____

_____

PROGRAM APPROVAL

By signing below, the undersigned, constituting all of the members of the *[board of directors]* or *[___ committee of the board of directors]* of Dealership, acknowledge the *[board's]* or *[committee's]* 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).

_____

_____

_____

_____

Attachment A

ACCOUNT IDENTIFICATION AND RISK ASSESSMENT WORKSHEETS

Instructions

NOTE: This set of Worksheets should be used only after proper modification and customization to suit each dealer's own circumstances. It is intended as a template or model to help you identify covered accounts and perform the necessary Risk Assessment to determine which business accounts should be included as covered accounts, and identify risk factors for each as required as part of the process of identifying relevant Red Flags.

This set of Worksheets should be used in conjunction with and pursuant to the ITPP. To use the Worksheets, review Section 5 of the ITPP, and follow the following steps:

- Consider each Dealership department (e.g., new-car sales, parts, service, etc.) working with the relevant managers.
- Within each department:
    - Consider each customer type.
    - Consider each account offered.
    - Consider each account maintained.
- Complete a mini-form as shown below for each type of account offered or maintained in that department for each customer type, listing the following:
    - The methods provided by the Dealership to open and, if applicable, maintain the account
    - The Dealership's own previous identity theft experience with respect to that type of account
- Use this information to perform the Risk Assessment to determine if certain types of non-consumer accounts should be deemed covered accounts. (Note: Multiple-payment consumer accounts must be identified as covered accounts. However, as discussed above on pages 5-6, single-payment consumer or "other" accounts may be covered accounts if they involve a continuing relationship.)
- Reflect the results of that determination in the final check box for each account Worksheet.
- NOTE: This information will also be used in the process of identifying relevant Red Flags.
- Do the same for all remaining customer types and accounts in that department.
- Repeat the process for each department.
- Include the results in Section 9 of the ITPP.

The Worksheets in the following pages include a blank form to be filled in by the Dealership in analyzing each of its accounts, as well as sample completed templates for a series of accounts that may be encountered by dealers. Review these carefully, keeping in mind that they are examples, and that you should apply the process above to your own dealership. In addition to the accounts listed, you should complete a Worksheet and analyze any other extension of credit or deferred payment program that includes a continuing relationship.

ACCOUNT IDENTIFICATION AND RISK ASSESSMENT WORKSHEET

TEMPLATE

Department(s): _____

Customer Type: _____

Account: _____

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1._____

2. _____

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1._____

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ❑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:
❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

❑ YES ❑ NO

ACCOUNT IDENTIFICATION AND RISK ASSESSMENT WORKSHEETS

EXAMPLE A

Department(s): *New- and Used-Car Sales*

Customer Type: *Consumer (personal, family, household)*

Account: *Retail installment sale contract*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *In-person credit application and retail delivery at the Dealership*
2. *Online/telephone credit application; in-person execution of contract; and retail delivery at the Dealership*
3. *Online/telephone credit application; off-site delivery*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ☑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ❑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

EXAMPLE B

Department(s): *New- and Used-Car Sales*

Customer Type: *Consumer (personal, family, household)*

Account: *Vehicle lease*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

Same as "Example A"

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

Same as "Example A"

a. ☑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ❑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

EXAMPLE C

Department(s): *New- and Used-Car Sales*

Customer Type: *Business Customer (non-fleet)*

Account: *Installment sale contract*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

Same as "Example A"

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

Same as "Example A"

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ☑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

☑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

EXAMPLE D

Department(s): *New- and Used-Car Sales*

Customer Type: *Business Customer (non-fleet)*

Account: *Vehicle lease*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

Same as "Example A"

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

Same as "Example A"

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ☑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

☑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

ACCOUNT IDENTIFICATION AND RISK ASSESSMENT WORKSHEETS

EXAMPLE E

Department(s): *Parts, Service, Body Shop*

Customer Type: *Business*

Account: *Open book account to charge purchases for repair shops and similar businesses*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *Available only after long-standing, successful c.o.d. relationship and only for parts or service purchases rendered to vehicle registered in customer's business name or, for parts purchases, where parts are delivered by the Dealership to the customer's established business location*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ☑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

❑ YES ☑ NO

***NOTE: You may consider separate Worksheets for Parts, Service, and Body Shop if the available methods for opening such accounts differ by department.**

EXAMPLE F

Department(s): *Parts, Service, Body Shop*

Customer Type: *Business*

Account: *Receivable account for warranty or service contract parts and labor provided to manufacturer or service contract obligor*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *Available only pursuant to extensively reviewed and formalized dealer sales and service agreement, or service contract provider agreement, and accessible only through secure claims authorization system, and limited to parts or service for specific vehicle, identified by VIN, covered by warranty or service contract*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ☑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

❑ YES ☑ NO

EXAMPLE G

Department(s): *Daily Rental Car*

Customer Type: *Business*

Account: *Open book account to charge daily rentals for use by local businesses*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *Available in very few instances and only pursuant to extensively reviewed and formalized agreements*
2. *Accessible only through direct communication between owner of the business and Dealership's rental car manager*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ❑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ☑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

❑ YES ☑ NO

EXAMPLE H

Department(s): *Service and Parts*

Customer Type: *Consumer (personal, family, household)*

Account: *Customer charge account issued by the Dealership*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *Available only rarely, in limited instances, for repeat, high-volume customers with whom the Dealership has a long history and a great deal of familiarity. Written approval of the department manager required.*
2. *Accessible only through direct communication between department manager and specific individual*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ☑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ❑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

ACCOUNT IDENTIFICATION AND RISK ASSESSMENT WORKSHEETS

EXAMPLE I

Department(s): *Service, Parts, Body Shop, Car Rental*

Customer Type: *Consumer (personal, family, household)*

Account: *Dealership-issued employee charge accounts*

METHODS PROVIDED BY DEALER TO OPEN OR ACCESS THIS ACCOUNT

1. *Available only to Dealership employees who have been employed more than one year. Access to the account is only via the Dealership payroll department, with approval of the department manager.*

DEALERSHIP'S PREVIOUS ID THEFT EXPERIENCES WITH THIS ACCOUNT

1. *None Identified*

a. ☑ This is a consumer account involving multiple payments or transactions. (If checked, skip to item c and check "Yes.")

b. ❑ This is an "other account." (If checked, complete Risk Assessment below.)

Risk Assessment:

❑ After appropriate consideration of the above and other facts, the Dealership has determined that this account poses a reasonably foreseeable risk to customers or to the safety and soundness of the Dealership from identity theft. (If checked, skip to item c and check "Yes.")

c. This is a covered account.

☑ YES ❑ NO

Attachment B

RED FLAG IDENTIFICATION, DETECTION, AND RESPONSE WORKSHEETS

Introduction

NOTE: Use of these Worksheets is not appropriate without proper modification and customization to suit each dealer's own circumstances. Both the template and the examples below are offered only to aid in the creation of a list of Red Flags that are relevant to your dealership.

Closely review the Red Flag Identification, Detection, and Response Worksheet Template, the sample Worksheets, and the sample ITPP (Sections 7 and 8) to develop your list of relevant Red Flags. Then take the following steps:

1. Begin by completing a Worksheet for each of the 26 FTC Example Red Flags found at Supplement A to Appendix A of the Red Flags Rule and included in this Attachment;
2. Then complete Worksheets for any other relevant Red Flags you have identified.
3. Once you have completed a Worksheet for all Red Flags:
    a. List/incorporate in Section 10 of the ITPP those Red Flags you have deemed "relevant."
    b. List/incorporate in Section 11 of the ITPP the methods you have identified to detect those Red Flags.
    c. List/incorporate in Section 12 of the ITPP the specific responses you have identified upon detection of a relevant Red Flag.

Below, you will find a series of completed Worksheets for a hypothetical sample dealership. Included are Worksheets for the 26 Example Red Flags, followed by several dealership-specific Red Flags that are not contained on the FTC's list. These dealership-specific Red Flags are similar to certain Example Red Flags, but have been tailored to more accurately reflect a typical dealership's circumstances. You may consider whether the dealership-specific Red Flags below, or something similar, may be appropriate for your dealership.

Please note that the relevance determinations reflected in the sample Worksheets are based on the following assumptions about the sample dealership:

1. The only "covered accounts" offered or maintained by the sample dealership are motor vehicle installment sale and lease accounts.
2. The sample dealership immediately assigns those accounts to third-party finance sources.
3. The sample dealership opens accounts only via in-person meetings with the customer where in-person identification procedures may be conducted.

As a result, all Red Flags concerning open-end lines of credit and improper account access are deemed irrelevant to this sample dealership. Your relevance determinations may be different; please tailor the Worksheets to your dealership's circumstances.

TEMPLATE

RED FLAG:	_____
APPLICABLE ACCOUNT(S): _____	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ❑ **NO**	

Detection Method(s)
(Complete if "yes" box is checked.)

1. _____
2. _____

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. _____
3. _____

WORKSHEET INSTRUCTIONS

RED FLAG:	_____ (#1 below)
APPLICABLE ACCOUNT(S): _____ (#2 below)	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG **❑ YES** **❑ NO** (#3 below)	
Detection Method(s) (Complete if "yes" box is checked.) 1. _____ (#4a below) 2. _____ **Response(s)** 1. Follow the general response procedures in Section 12 of the ITPP. (#4b below) 2. _____ 3. _____	

1. Describe or identify each Red Flag.
2. Identify the covered accounts to which this Red Flag applies.
3. Check the appropriate box to indicate whether this Red Flag is relevant (based on the guidance contained in Section 7 of the ITPP).
4. If the Red Flag is deemed "relevant" ("Yes" box checked):
    a. List appropriate method(s) for detecting that Red Flag.
    b. List appropriate specific response procedures, if any, once that Red Flag is detected (in addition to the general response procedures contained in Section 12 of the ITPP).
5. Once all Worksheets are complete:
    a. List all relevant Red Flags from all Worksheets in Section 10 of the ITPP.
    b. Gather all the detection methods identified, remove the duplicates, and incorporate them into the detection procedures in Section 11 of the ITPP.
    c. Gather all of the specific response procedures, remove the duplicates, and list them as Specific Response Procedures in Section 12 of the ITPP.

THE 26 FTC EXAMPLE RED FLAGS:
IDENTIFICATION OF METHODS OF DETECTION AND SPECIFIC RESPONSE

CATEGORY ONE: "Alerts, Notifications, or Warnings from a Consumer Reporting Agency"

RED FLAG 1	A fraud or active duty alert is included with a consumer report.

APPLIES TO: The opening of all covered accounts where a consumer is liable

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain a consumer report.
    A. Check for a fraud or active duty alert.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. Do not open the account 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 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 the ITPP.
    D. Prepare and sign a written acknowledgment detailing how each of the above steps was completed.

RED FLAG 2	**A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.**

APPLIES TO: The opening of all covered accounts where a consumer report is obtained

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

1. Before opening the account, obtain a consumer report.

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

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

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

RED FLAG 3	**A consumer reporting agency provides a Notice of Address Discrepancy.**

APPLIES TO: The opening of all covered accounts where a consumer report is obtained and a Notice of Address Discrepancy is received

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

1. Before opening the account, obtain a consumer report.

    A. Be alert for notice from the credit reporting agency of an address discrepancy.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Do not open the account unless and until the Notice of Address Discrepancy Policies and Procedures in the ITPP are completed and the identity of the consumer is verified.

RED FLAG 4	**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; (d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.**

APPLIES TO: The opening of all covered accounts where a consumer report is obtained

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

1. Before opening the account, obtain a consumer report.

    A. Review the report for unusual or inconsistent activity.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. Ask the customer to explain the unusual activity.

RED FLAG 5	**Documents provided for identification appear to have been altered or forged.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes"box is checked.)

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.

    A. If involving a legal entity, obtain, inspect, and photocopy documents demonstrating the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

2. 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.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. 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 additional documentation to allow you to form a reasonable belief that the customer is who he or she claims to be. This may include requiring 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.

RED FLAG 6	**The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

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.

   A. Review the photo and physical appearance information on the identification and compare it with the consumer's in-person appearance.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Do not open the account unless a reasonable explanation for the discrepancy that is not indicative of identity theft is identified 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.

RED FLAG 7	**Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

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.

2. Before opening the account, obtain customer's signed credit application.

    A. Compare the address and other information on the identification with information provided by the consumer in the credit application.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Do not open the account unless a reasonable explanation for the discrepancy that is not indicative of identity theft is identified.

RED FLAG 8	**Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG **❑ YES** **☑ NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 9	**An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.**
APPLIES TO: The opening of all covered accounts	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG **☑ YES** **❑ NO**	
Detection Method(s) (Complete if "yes" box is checked.) 1. Before opening the account, obtain customer's signed credit application. A. Review the credit application for signs of alteration or forgery. **Response(s)** 1. Follow the general response procedures in Section 12 of the ITPP. 2. Ask customer to explain the apparent alteration.	

CATEGORY THREE: "Suspicious Personal Identifying Information"

RED FLAG 10	**Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example, (a) the address does not match any address in the consumer report; or (b) the Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG (SEE RED FLAG D1, below.) ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 11	**Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG (SEE RED FLAG D2, below.) ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 12	Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example, (a) the address on an application is the same as the address provided on a fraudulent application; or (b) the phone number on an application is the same as the number provided on a fraudulent application.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG. (SEE RED FLAG D3, below.) ❑ YES ☑ NO	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 13	Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. 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.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG (SEE RED FLAG D4, below.) ❑ YES ☑ NO	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 14	The SSN provided is the same as that submitted by other persons opening an account or other customers.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 15	The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 16	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain customer's signed credit application.

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

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Require the customer to provide the missing information. If he or she does not or cannot, do not open the account unless a reasonable explanation that is not indicative of identity theft is identified explaining why the requested information is missing or incomplete.

RED FLAG 17	**Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.**

APPLIES TO: N/A

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

❑ **YES** ☑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

RED FLAG 18	**For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

CATEGORY FOUR: "Unusual Use of or Suspicious Activity Related to the Covered Account"

RED FLAG 19	**Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 20	**A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example, (a) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or (b) the customer fails to make the first payment or makes an initial payment but no subsequent payments.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 21	**A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example, (a) nonpayment when there is no history of late or missed payments; (b) a material increase in the use of available credit; (c) a material change in purchasing or spending patterns; (d) a material change in electronic fund transfer patterns in connection with a deposit account; or (e) a material change in telephone call patterns in connection with a cellular phone account.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 22	**A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 23	Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 24	The financial institution or creditor is notified that the customer is not receiving paper account statements.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

RED FLAG 25	The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

CATEGORY FIVE: "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"

RED FLAG 26	**The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.**
APPLIES TO: N/A	
INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG (See Red Flag D5, below.) ❑ **YES** ☑ **NO**	
Detection Method(s) (Complete if "yes" box is checked.)	

DEALER-SPECIFIC RED FLAGS

The following Red Flags are tailored specifically to the dealer context. Where indicated, some of these Red Flags are derived from the FTC Example Red Flags and modified to be made potentially relevant to a dealership's Identity Theft Prevention Program.

RED FLAG D1	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG
NOTE: This is a modified form of Example Red Flag No. 10.

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain customer's signed credit application.

2. Before opening the account, obtain a consumer report.

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

3. Review the consumer report for warnings, notifications, or alerts concerning a mismatch between data supplied by the customer and data available to the consumer reporting agency.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Ask customer to explain the mismatch.

RED FLAG D2	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG
NOTE: This is a modified form of Example Red Flag No. 11.

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain customer's signed credit application.

    A. Review the address and other information on the credit application for consistency with other information provided in the credit application and other written information submitted by the customer.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

2. Ask customer to explain the mismatch.

RED FLAG D3	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG
NOTE: This is a modified form of Example Red Flag No. 12.

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain customer's signed credit application.
2. Before opening the account, obtain a consumer report.
3. Review the consumer report for warnings, notifications, or alerts concerning known or suspected fraudulent activity.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

RED FLAG D4	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG
NOTE: This is a modified form of Example Red Flag No. 13.

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Before opening the account, obtain customer's signed credit application.

2. Before opening the account, obtain a consumer report.

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

3. Review the consumer report for warnings, notifications, or alerts concerning potential fraudulent activity, such as warnings of suspect types of addresses.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.

RED FLAG D5	**The dealership is notified by a customer, a financial institution with which dealership does business, a victim of identity theft, a law enforcement authority, or any other person that that a potential identity thief may attempt to open an account with dealership using someone else's personal identifying information.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG
NOTE: This is a modified form of Example Red Flag No. 26.

☑ **YES** ❑ **NO**

Detection Method(s)
(Complete if "yes" box is checked.)

1. Make all F&I and sales desk personnel aware of notifications of potential identity theft attempts.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. Contact the individual who notified the dealership of the potential identity theft attempt to determine whether an attempted identity theft is occurring.
3. Consult with the Program Coordinator/Compliance Officer to determine whether law enforcement should be contacted.

RED FLAG D6	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

1. Open the account with the assumption that the execution of documents and delivery of the vehicle will occur on-site, at the dealership's facility. Be alert to any effort by the customer to request or steer the transaction toward an off-site delivery.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. Advise customers inquiring about off-site delivery that all paperwork, credit report, and identification procedures used by the 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.

RED FLAG D7	**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.**

APPLIES TO: The opening of all covered accounts

INCLUDED IN DEALERSHIP'S PROGRAM AS A RELEVANT RED FLAG

☑ **YES** ❑ **NO**

Detection Method(s)

(Complete if "yes" box is checked.)

1. Open the account with the assumption that the execution of all documents and delivery of the vehicle will occur on-site, at the dealership's facility. Be alert to any transaction where the co-buyer or co-lessee is not present or any effort by the customer to request or steer the transaction toward having the co-buyer or co-lessee sign documents off-site.

Response(s)

1. Follow the general response procedures in Section 12 of the ITPP.
2. 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.

OTHER DEALERSHIP-SPECIFIC RED FLAGS

Continue the analysis by completing Worksheets for any other Red Flags that are applicable to your dealership. Examples may include:

- Customer is reluctant or refuses to remove identification document from wallet, pocketbook, etc.
- Customer is reluctant or refuses to allow identification document to be copied or its magnetic stripe swiped according to dealership's standard procedures for doing so.
- Customer is reluctant or refuses to provide a thumbprint or be photographed according to dealership's standard procedures for doing so.
- Customer provides local residence and work addresses, but presents an out-of-state driver's license or other government-issued identification.
- Customer claims to be a referral from a prior customer and dealership now suspects the prior customer may have engaged in improper or fraudulent conduct.
- Customer seeks to purchase or lease multiple vehicles at one time for personal use.
- Customer makes statements suggesting the vehicle will be used by others who are not parties to the contract or lease.
- Customer asks that contract, lease, or title paperwork reflect an address other than addresses shown on the identification documents or consumer report.
- Customer's trade-in vehicle is titled or registered in someone else's name.
- Customer's down payment check is written on someone else's account.

Appendix A

SAMPLE CLAUSES TO INCLUDE IN SERVICE PROVIDER AGREEMENTS

One example the FTC provides of steps you may take under the Red Flags Rule to oversee your service provider arrangements is to require contractually each service provider who performs activities in connection with covered accounts to have policies and procedures in place to detect relevant Red Flags and, if detected, to respond appropriately. Appropriate contractual provisions to this effect could be included in a free-standing agreement with the service provider, in an amendment to an existing agreement with the service provider, or in an addendum to the service provider's standard agreement. The sample clauses below, while suitable for inclusion in any of these, are offered for illustrative purposes only and should not be used absent a thorough review of all facts pertaining to your retention of the service provider and consultation with your attorney.

Sample 1 would be most appropriate for service providers who do not have their own identity theft prevention programs and who would not be expected to create comprehensive policies and procedures to combat identity theft. This category of service provider might include sole proprietors, such as vehicle brokers, who take some role in the account opening process. In essence, Sample 1 "deputizes" the service provider as one of your staff for purposes of the ITPP.

Sample 2 is more appropriate for service providers who are familiar with and capable of creating and implementing formal internal policies and procedures, or who might be reluctant or unwilling to pledge allegiance to your ITPP.

SAMPLE 1 – Service Provider Required to Follow Your ITPP

"Service Provider acknowledges that Service Provider has received and reviewed a copy of the written Identity Theft Prevention Program (ITPP) maintained by Dealership pursuant to the FTC Red Flags Rule, 16 C.F.R. §681.2. In performing activities in connection with a Covered Account (as defined in the ITPP), Service Provider and its personnel will observe and comply with all terms and provisions of the ITPP and with all instructions issued pursuant to the ITPP by the Program Coordinator and Compliance Officer identified in the ITPP."

SAMPLE 2 – Service Provider to Maintain and Follow Provider's Own ID Theft Policies

"Service Provider acknowledges that Service Provider has received and reviewed a copy of the written Identity Theft Prevention Program (ITPP) maintained by Dealership pursuant to the FTC Red Flags Rule, 16 C.F.R. §681.2. In performing activities in connection with a Covered Account (as defined in the ITPP), Service Provider and its personnel will maintain and observe policies and procedures to detect relevant Red Flags that may arise in the performance of the Service Provider's activities, and will take appropriate steps to prevent or mitigate identity theft. Service Provider agrees to report promptly and comprehensively to Dealership in writing in the event Service Provider in connection with a Covered Account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that Service Provider detects in connection with a Covered Account."

Appendix B

SAMPLE COMPLIANCE REPORT

The language that appears in the template below is intended to assist dealers with the preparation of compliance reports that the Red Flags Rule requires dealership staff to submit to the dealership board of directors, an appropriate board committee, or a designated senior management employee on at least an annual basis. The template refers to three exhibits (A, B, and C) which do not appear in this publication and which your dealership would have to prepare if it chooses to adopt this reporting format. The template language that appears below is offered for illustrative purposes only. Consult your attorney concerning the language that your dealership should use to satisfy its reporting obligation.

Annual [or Special] Report on The Identity Theft Prevention Program of [Dealership Name]

Pursuant to Section 17 of the Identity Theft Prevention Program (ITPP) adopted by [Dealership Name] (Dealership), this report ("Report") is submitted to the Compliance Officer [*or board of directors, a board committee, or other member of senior management*] by the Program Coordinator and staff responsible for the development, implementation, and administration of the ITPP. This Report is intended to support and strengthen the ITPP and comply with its reporting requirements.

1. ITPP Adoption and Implementation

The ITPP was approved by the board of directors on _____, and became effective on November 1, 2008.

As reflected by written attendance records and signed acknowledgment forms reviewed by the Program Coordinator, all Dealership employees having duties with respect to account opening or maintenance have received training under the ITPP and have agreed to abide by its terms. In addition, all new employees with such duties receive training under the ITPP and sign acknowledgments agreeing to comply with its terms during the orientation process.

[If there has already been a Report, add: Prior to this Report, the most recent Report prepared by the Program Coordinators respecting the ITPP was dated and submitted to the Compliance Officer on _____.]

[If there have been any amendments to the ITPP since the last Report, add: The most recent amendment to the ITPP was adopted and dated _____.]

2. ID Theft Experience and Awareness Log

Attached to this Report as Exhibit "A" is a copy of the current ID Theft Experience and Awareness Log maintained by the Program Coordinator. The log lists all incidents involving identity theft at the Dealership occurring since the effective date of the ITPP [or *date of the last Report*], as well as a description of methods of identity theft Dealership has identified since that time that reflect changes in identity theft risks.

[Insert here a summary of each incident of identity theft reported on the log and for each incident describe the response taken by management of the Dealership.]

3. Regulatory Guidance

Prior to preparing this Report, the Program Coordinator reviewed all Red Flags Rule materials at www.ftc.gov and took other reasonable steps to identify applicable supervisory guidance by the FTC and other relevant regulatory agencies respecting identity theft detection, prevention, and mitigation. Relevant guidance and other information so obtained are summarized in Exhibit "B" attached to this Report.

4. Service Provider Arrangements

For each service provider performing activities in connection with the Dealership's covered accounts, Exhibit "C" lists the service provider's name, the nature of the activities performed by the service provider in connection with covered accounts, and the date a written agreement or contract was signed by the service provider wherein the Dealership required the service provider 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.

[Here, the Program Coordinator should offer an evaluation of how the service provider arrangements are working, such as: "The Dealership has relatively few arrangements with service providers, and all have executed the contractual provisions required by the ITPP. All service providers appear to be in compliance with these contractual obligations."]

5. Other Material Issues Related to the ITPP

In addition to the matters listed on the current ID Theft Experience and Awareness Log (Exhibit A), the following material issues arose in connection with the ITPP since its inception [or *since the most recent prior Report*]:

[Since Exhibit A reflects actual identity theft experiences, and Exhibit B reflects legal and regulatory developments, this section will most likely be limited to administrative and management issues under the ITPP, such as "the Program Coordinator needs an assistant."]

6. Evaluation of Effectiveness of ITPP

After considering the information identified above, the Program Coordinator offers the following evaluation of 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:

[Here, include the Program Coordinator's evaluation, such as: "The absence of any material identity theft incident suggests that the policies and procedures set forth in the ITPP are effective at the present time in addressing the risk of identity theft."]

7. Recommendations for Changes to the ITPP

In addition, the following represents the conclusion of the Program Coordinator with respect to whether there is a need to make changes to the ITPP:

[Here, include the Program Coordinator's conclusion and rationale, such as: "At this time, the effectiveness of the existing policies and procedures and absence of any material developments in the other areas discussed in this Report suggest that no material changes to the ITPP are necessary at this time."]

Respectfully submitted,

_____ _____

Date Program Coordinator

NOTES

NOTES

NOTES

ACKNOWLEDGMENT

This management guide was prepared for NADA by

Halbert B. Rasmussen, Esq.
Manning, Leaver, Bruder & Berberich
5750 Wilshire Boulevard, Suite 655
Los Angeles, California 90036

NADA-ATD
Resource Toolbox

National Automobile Dealers Association
8400 Westpark Drive
McLean, Virginia 22102-3591

http://www.NADAuniversity.com

ATD
AMERICAN TRUCK DEALERS
A DIVISION OF NADA