ATTENTION DEALER PRINCIPAL or MANAGING EXECUTIVE
Congratulations! You have taken the first and most important step towards satisfying the requirements of the Red Flags Rule.

Important Notice
In order to properly implement your Identity Theft Protection Program, you must carefully read and follow the steps outlined in this handbook. It is recommended that you keep a copy of this handbook in your DealerAide Nonpublic Personal Information Compliance Binder for reference. It will also be helpful during periodic audits and employee training.

DISCLAIMER: Your DealerAide Nonpublic Personal Information Compliance Program is not legal advice and does not create an attorney-client relationship between any purchaser or user and David N. Robertson, Member Benefits Services, Inc., the Association of Finance & Insurance Professionals, their employees or contractors, or the company or individual who recommended it. The program and all forms, procedures, and resources should be reviewed by competent legal counsel before use to ensure their applicability to each dealer’s unique circumstances. The Identity Theft Prevention Program materials reflect the authors’ interpretation of the measures that should be in place to comply with the Red Flags Rule. It is the responsibility of the user to implement customized procedures and actively maintain, enforce, and update the program.

Your DealerAide Nonpublic Personal Information (NPI) Compliance Program is divided into two parts: 1) the Information Security Program (ISP), which covers the Safeguards Rule and the Disposal Rule; and 2) the Identity Theft Prevention Program (ITPP), which covers the Red Flags Rule. Both your ISP and ITPP include: A) Rule implementation handbooks, B) Customized portions of your ISP and ITPP created with the Online Template Generator, C) Conference-call orientation sessions, and D) Online forms, tools, and resources. The Quick-Start Guide, the ISP, and the ITPP should be kept in your NPI Compliance Binder.
About The Red Flags Rule

The Red Flags Rule is a critical component in the continuing crusade to curb identity theft. The Gramm-Leach-Bliley Act (GLB) was enacted to address the disposition and protection of Nonpublic Personal Information (NPI). The Financial Privacy Rule of November 2000 mandated that consumers be informed of how their NPI will be used by certain businesses.

The Safeguards Rule, effective May 2003, required those who collect NPI – in either electronic or paper format – to protect it from theft or compromise. The Red Flags Rule is a natural and necessary extension of that legislation. The Red Flags Rule requires creditors (and at the time the sale is being consummated, your dealership is a creditor) to take steps to validate that the customer is who they say they are. A “Red Flag” is a suspicious circumstance, pattern, practice, or specific activity that indicates the possibility of identity theft. It is a set of clues, such as address discrepancies or other inconsistencies, which help detect, and can lead to the prevention and mitigation of, identity theft.

About the Identity Theft Prevention Program

The Identity Theft Prevention Program (ITPP) is one of two parts of the DealerAide NPI Compliance Program. The ITPP is designed to help dealerships comply with the requirements imposed by the Red Flags Rule. The other part of the compliance program, the Information Security Program (ISP) covers the Safeguards Rule and the Disposal Rule.

One size does not fit all, which is why we provide a customized program with modifiable documents that allow you to tailor the recommended policies, procedures, and forms to suit your organization structure and operational capacity.

After you complete the Online Template Generator, customized documents are created that will become part of your ITPP. After modifying the customized documents to accommodate the structure of your dealership, print them and place them in the NPI Compliance Binder behind the proper tabs.

This handbook is also part of your ITPP. It provides a step-by-step guide to help you achieve the goals in your program. It references modifiable procedures and online forms that should be customized according to your organization’s particular structure and included in the NPI Compliance Binder. For your convenience, the handbook and forms can be downloaded online. The website also contains resources, sample forms, and collateral material to support and supplement your ITPP.

Throughout the text, we offer practical comments to help you implement your new ITPP. You will find a wealth of information to cover many contingencies. We hope the DealerAide NPI Compliance Program will establish the standard for compliance throughout the retail automobile, RV, and motorcycle industries.

For Assistance
If you have questions about the procedures herein, contact:
David N. Robertson, President
Member Benefits Services, Inc.
817.248.2434
david.robertson@afip.com
For regulatory assistance, please contact your corporate counsel.
DEFINITIONS

The following is a list of terms you must understand to complete the Online Template Generator and implement the ITPP portion of your DealerAide Nonpublic Personal Information Compliance Program.

**Address Discrepancy Form** – in certain situations Experian, TransUnion, or Equifax will issue an address discrepancy notice requiring the dealer to collect and submit information that will aid in affirming the actual address of the person listed on the credit application. In such cases, a generic response form (interactive PDF) is available as an online resource to aid in preparing and responding to such a request - Address Discrepancy Form & Instructions.

**Periodic or Annual Report** – it is an ITPP requirement that periodically or annually (more often if required by circumstance – see corporate counsel for a recommendation), a report be drafted that notes any revisions or updates to the ITPP. At a minimum, the report should cover 1) how effective the current program has been in addressing the risk of identity theft; 2) how effective it has been at monitoring the practices of Service Providers and any changes to the Service Providers employed and/or their Red Flags Rule-related policies and procedures; 3) Incident Reports, especially those incidences that resulted in an actual identity theft, and your responses; and 4) recommendations for changes to the ITPP (including personnel changes). It should include changes in policies and procedures and any personnel changes (e.g., a different person was appointed as the Corporate Compliance Officer). It should also contain evidence that newly appointed company employees responsible for supporting the ITPP have been properly oriented (the training verification form should be signed and filed for each person). The final compilation of information and supporting material is to be presented for formal Board of Directors approval (it is recommended that a qualified lawyer affirm that it meets the requisites of the Red Flags Rule) with the copy of the written approval placed in the NPI Compliance Binder.

**Buyer** – the individual, individuals, or corporate entity attempting to lease or purchase and/or to secure the funding for the purchase of any item or items within the scope of the Red Flags Rule (vehicles, RVs, motorcycles, boats, trailers, major dollar amount parts such as crate engines, accessories or supplemental equipment, or in some cases, service). The term includes customers, co-buyers and/or co-signers.

**Buyer’s Order** – refers to the document signed by the Buyer and dealer that reflects the agreed-to dollar amounts and specific terms of the item designated for purchase, possible funding, and owner indemnification. (See Purchase Order)

**Challenge Question** – asks a Buyer to recall information to a personal question in an attempt to confirm their identity (e.g., mother’s maiden name, former employers or former home addresses, dollar amount of remaining mortgage, etc.). Special care should be taken when using Challenge Questions to use Out-of-Wallet information (information not readily available if the Buyer is an identity thief in possession of a stolen wallet – see below). The Customer Contact Representative employing this device should choose a question to which he/she knows the answer as a result of a document obtained by the dealer with the Buyer’s information (e.g., credit history report) and not information provided by the Buyer (e.g., credit application).

**In-Wallet Information** – Information that could be found in someone’s wallet (Driver’s License number, home address, place of employment, etc.)
Out-of-Wallet Information – Information that is unlikely to be found in someone’s wallet (former home addresses, former places of employment, remaining dollar amount of existing mortgage, etc.)

Contract – installment sale agreement or consumer lease agreement.

Customer Contact Representative – the individual charged with obtaining the Buyer’s personal and credit history information for the purposes of completing a transaction for a Unit (often the F&I manager or salesperson).

Dealer – the individual, individuals, or corporate entity legally responsible for the activities of the organization governed by the ITPP, the store (dealership).

Driver’s License – typically refers to the actual state-issued license required to operate a motor vehicle, but in cases in which the Buyer, co-buyer or co-signer does not possess this form of identification and does not require the ability to legally drive to participate in the transaction, it also refers to any valid (non-expired) government-issued photo-bearing identification legally acceptable as formal identification by the government (e.g., state-issued ID, military ID).

DeskCheck – the Red Flag F&I DeskCheck© (included with your DealerAide: Nonpublic Personal Information Compliance Program) or any Dealer-produced or obtained document that describes the processes employed by the Customer Contact Representative to gather necessary information and confirm the identity of the Buyer. The purpose of this process is to make a determination of whether any Red Flags exist based on the information readily available on the documents initially received by the Customer Contact Representative. Failure to meet the full requirements of the DeskCheck indicates a possible or actual Red Flag and the Customer Contact Representative must follow the steps indicated by the ITPP in an attempt to clear the Red Flag.

Nonpublic Personal Information (NPI) Compliance Binder: This is the binder that comes with your DealerAide NPI Compliance Program. It has tabs to help you organize your materials for easy reference and documentation of compliance with the rules. You will need a separate DealerAide NPI Compliance Program and binder for each facility in your company. The Facility Compliance Officer for each facility will maintain the NPI Compliance Binder for their separate location. The Corporate Compliance Officer will maintain a separate binder containing the compliance material for every facility. If necessary, additional binders can be purchased for a nominal fee.

Incident Report – an internal document to be completed and filed in the NPI Compliance Binder when 1) an open Red Flag cannot be cleared and as a result the deal is not consummated (whether or not an actual identity theft occurs) or 2) an actual identity theft occurs. The report will include the written affidavits (detailing the pertinent facts) prepared by the individuals involved in the situation in an official capacity (as applicable, Dealer principal, legal advisors, Corporate Compliance Officer, Red Flags Coordinator Customer Contact Rep, Service Provider officials, credit bureau officials, law enforcement personnel, or any other individual with relevant information). Included with the report should be copies of the Buyer’s Order, credit application, all credit bureau-issued material, and all material issued by the relevant Service Provider. (Not a substitute for a Suspicious Activity Report.)
**Red Flags Policy:** A component of the ITPP that outlines the general procedures by which the dealership will detect, prevent, and mitigate Identity Theft as required by the Red Flags Rule. The Red Flags Policy is created using the Online Template Generator and should be modified for the specific needs of your dealership.

**Red Flags Rule:** A regulation issued by the FTC (16 CFR 681, effective December 31, 2010) requiring the detection, prevention, and mitigation of Identity Theft by certain creditors, including automobile dealers.

**Purchase Order** – A Buyer-generated document giving authority to purchase to a representative of the Buyer. The same standards apply to a Purchase Order as to a Buyer’s Order.

**Service Provider** – a lender, vendor, or third-party provider of dealership-related services used by Dealer during the course of leasing, selling, or obtaining funding for a Unit (e.g., captive or institutional lender, lending portal, aftermarket product provider, etc.). The specific tasks handled by certain such providers may require modification to Dealer ITPP. (See Service Provider ITPP Agreements provided as an online resource.) Dealer is not absolved of responsibilities under the Red Flags Rule because outside Service Providers are used.

**Suspicious Activity Report (SAR)** – a form to be filed with the Treasury Department in the case that a Dealer, as a possible money services business under 31 USC 5312(a)(2)(T) and in accordance with 31 USC 5318(g), knows or suspects that:

- The funds come from illegal activity or disguise funds from illegal activity;
- The transaction is structured to evade Bank Secrecy Act (BSA) requirements or appears to serve no known business or apparent lawful purpose; or,
- The Money Service Business (MSB) is being used to facilitate criminal activity.

**Unit** – any physical item available for sale or lease in a dealership (e.g., cars, trucks, equipment, trailers, boats, RVs, motorcycles, watercraft, etc.)
An F&I Manager’s Role

The information provided in this guide is not legal advice, rather, it is a practical way for F&I managers to understand their role under the Red Flags Rule. Their role is not to determine the exact identity of customers, but to verify that they are who they claim to be. Their job is not to determine whether someone is actually an identity thief – their title is “F&I manager,” not “Detective.”

Every customer will have some gaps in their paper trail (most of which aren’t their fault), but most customers are legitimate, so being accusatory or suspicious because of an inconsistency could send legitimate customers to a dealership down the street. Treat customers with respect at all times.

The role of the F&I manager is limited to collecting and clarifying customer information. Your primary duties are to secure the funding and sell aftermarket products. If you find any inconsistencies that require authentication beyond securing and clarifying information, you should turn the matter over to someone further up the chain of command (more on that later).

The dealer’s Identity Theft Prevention Program (ITPP) is designed to detect, prevent, and mitigate identity theft. It should be treated as a customer benefit because it protects consumers from identity theft.

Accountability

The dealership is ultimately accountable for complying with the Red Flags Rule, regardless of who is responsible to perform designated tasks in the ITPP, but you can (and should) be held accountable by your supervisor. This guide is based on a system in which in-store personnel perform the functions mandated by the Red Flags Rule. However, your dealership may have one or more service providers that handle some or all of these duties. If that is the case, your responsibilities in dealing with those vendors or using their services should be outlined in the dealership’s ITPP.

The Red Flags Rule applies to creditors who originate or maintain covered accounts – which can include consumer credit sale and lease transactions, buy-here/pay-here accounts, commercial/fleet credit sale and lease transactions, and commercial parts/service accounts (for a complete explanation the Red Flags Rule section 16 CFR 681.1 is available as an online resource).

The Red Flags Rule requires that your ITPP be in writing and approved by the board of directors (or a person or entity that performs a similar function). This requirement imposes an ethical and legal duty on the dealership for implementation, application to daily operations, annual reporting, and updating requirements. It is strongly recommended that the dealership’s ITPP be approved in writing by a competent attorney prior to board approval.
Penalties

As with the Safeguards Rule, simply not having an ITPP in place will constitute a violation of the Red Flags Rule, whether or not a Red Flag is detected or identity theft has been attempted or committed. The administrative penalty for violating the Red Flags Rule is $2,500 per violation.

It is not clear what the FTC will consider a single violation, however, based on the agency’s enforcement of the Safeguards Rule, some industry lawyers believe that every sale or lease transaction that occurs in the absence of a properly implemented ITPP could be treated as a separate violation (thus, if you sell 200 cars without complying with the rule, you could be fined as much as $500,000). Dealerships that violate the Red Flags Rule may also be subject to state laws that prohibit “unfair and deceptive acts and practices.”

The relatively low cost of complying with the Red Flags Rule by using one of the many program-building tools on the market (see AFIP’s website for an example) makes noncompliance an unnecessarily expensive mistake.

Identity Theft Prevention Program Overview

The Red Flags Rule is similar to the Safeguards Rule and Disposal Rule in that it requires dealerships to develop a compliance program and establishes minimum program standards. Each rule gives dealerships not only the flexibility to tailor the compliance program to their operation, but a directive to do so.

The Red Flags Rule mandates that each dealership establish an Identity Theft Prevention Program (ITPP), which outlines the steps a dealership and its personnel should take to:

- **IDENTIFY** Red Flags
- **DETECT** Red Flags
- **RESPOND** appropriately to Red Flags to **PREVENT** and **MITIGATE** identity theft
- **ADMINISTER** and **UPDATE** the program

The Red Flags Rule itself includes factors to consider when identifying the Red Flags that will be a key component of the program – the types of accounts the dealership maintains, sources and categories of Red Flags, and a list of suggested Red Flags. The Rule also provides suggested responses to Red Flags and guidelines for documenting, administering, and updating the program (the Red Flags Rule 16 CFR 681, Appendix A to Part 681, is available as an online resource).
If a dealership receives a notice of an address discrepancy from a consumer reporting agency or service, the original version of the Red Flags Rule required dealerships to provide that agency with the consumer’s correct address if the dealership is able to verify the address provided by the consumer (an Address Discrepancy Form and Instructions are available as online resources). This address discrepancy reporting requirement still applies to dealers but is now a separate regulation (the Address Discrepancy Rule section 16 CFR 641.1 is available as an online resource).

**Program Oversight and Staffing Structure**

The Red Flags Rule specifically mandates that either the board of directors, an appropriate committee of the board, or a designated employee at the senior management level assign an individual who will be responsible for the development, implementation, and ongoing management of the ITPP. This specific structure (unless otherwise indicated) is not required by the rule. It is simply an example of how it might work.

**Corporate Board of Directors** (or a governing body of equal stature)
The board of directors, an appropriate committee of the board, or a designated employee at the senior management level (hereafter referred to as “board”) will assign an individual to serve as the Corporate Compliance Officer. The board of directors will review and, on advice of competent counsel, approve the dealership ITPP. In addition, the board will review and approve all incident reports, all periodic or annual reports, and any revisions to the program.

**Corporate Compliance Officer**
The Corporate Compliance Officer will be responsible for the drafting, implementation, monitoring, and daily management of the ITPP including maintaining and updating the NPI Compliance Binder. This individual will prepare and submit for board approval (and legal review, when applicable) all incident reports, the required periodic or annual report, and any changes or updates to the ITPP.

The Corporate Compliance Officer reports to the dealer principal (or governing executive) and the board of directors periodically or annually and is the direct line manager over the Red Flags Coordinators and Customer Contact Representatives. This position will be equivalent to the Safeguards Rule Corporate Compliance Officer (and in many dealerships, will be the same person).

The Corporate Compliance Officer is also responsible for:

- responding to notices from credit reporting agencies, lending sources, Service Providers, customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts originated at the dealership;

- appointing qualified workers to serve as Red Flag Coordinators and Customer Contact Representatives, conducting the required training, and ensuring the documentation of the completion of the training;

- contacting the appropriate authorities in cases of suspected, attempted, or actual identity theft; and

- filing suspicious activity reports (SARs), if required.

**Red Flag Coordinators**
Because the Corporate Compliance Officer has multiple responsibilities under the Red Flags Rule, there’s a second tier position between that individual and the Customer Contact
Representatives. As such, the responsibility for applying the program’s policies and procedures to daily operations will fall to Red Flag Coordinators, who in turn, oversee and provide support for the Customer Contact Representatives. The Red Flag Coordinators are the mid-level managers (F&I directors, sales managers, comptrollers, or office managers) who are charged with responding to Red Flags discovered by Customer Contact Representatives and dictating courses of action. This structure provides a second level of review and a higher level of experience when evaluating response alternatives. The program should be structured to ensure that a Red Flag Coordinator is available for assistance during normal business hours.

The Red Flag Coordinator is also responsible for:

- applying the ITPP policies and procedures to daily operations as assigned to the Red Flags Coordinator;
- directing the actions of the sales personnel or F&I staff (Customer Contact Reps) as applicable when a Red Flag is detected or suspected and coordinating the activities until the Red Flag has been cleared or the incident is classified as an attempted or actual identity theft;
- preparing and filing an address discrepancy notice to a credit reporting agency when required; and
- conducting the administrative tasks associated with fraud or active duty alerts and credit freezes; and
- conducting Social Security card state of issue (or deceased persons) inquiries.

Customer Contact Representatives

The primary focus of the Customer Contact Representatives (F&I managers and staff) is to secure funding and sell aftermarket products. They should be responsible for collecting and clarifying information (performing the initial DeskCheck, ensuring the customer provides all the information, clarifying anything that doesn’t match up initially) and, if directed by the Red Flags Coordinator, securing additional information to further clarify the information provided by the customer. The Customer Contact Representative may also be responsible for updating the correct address if a credit reporting agency sends a notice of address discrepancy with a credit report and they are able to reasonably verify that an updated address is accurate. An Address Discrepancy Form and Instructions are available as online resources.

Customer Contact Representatives should not decide how to respond to Red Flags they cannot clear in the course of their normal duties. They should refer such matters to the Red Flags Coordinator without notifying the customer until instructed to do so.

Customer Contact Representatives are also the primary communication link between customers and the dealership’s contracted Service Providers, including funding sources, credit bureaus, credit brokers, or other third-party credit arrangers and credit card providers.

Red Flags Rule Policy & Program Drafting and Oversight Committee (optional)

A committee chaired by the Corporate Compliance Officer (and any upper-echelon executives so designated by the dealer principal) and staffed by the Red Flag Coordinators and Customer Contact Representatives will review the requisites of the Red Flags Rule and the information provided in this guide and other industry resources to develop an ITPP tailored to the dealership’s needs.
The committee should meet at least semiannually to evaluate current procedures and submit changes to the ITPP for review by competent counsel and for board approval. The oversight committee will assist the Corporate Compliance Officer with the drafting of incident reports and the preparation of the annual report.

**Identifying Applicable Red Flags**

The Red Flags Rule requires creditors who originate or maintain covered accounts to identify the Red Flags applicable to their particular operating environments. A Red Flag is a pattern, practice, or specific activity that indicates the *possible existence* of identity theft. A Red Flag doesn't mean an identity theft is in progress; it just means there's a discrepancy that *could be* an indicator of identity theft, and it's up to the dealership to verify the customer's identity.

The types of customer accounts a creditor processes and the methods for opening or maintaining them will influence the specific Red Flags that apply to a dealership and should be included in the ITPP.

The FTC lists examples of what may constitute a Red Flag in the rule. However, it recognizes that they won't all apply to every creditor and that other indicators may need to be added to a particular dealership's program. Also, the combination of several individual indicators may constitute a single Red Flag.

Among the Red Flags listed by the FTC, the following apply to typical credit transactions and were considered in developing the dealership-specific Red Flags suggested later in this section (the Red Flags Rule 16 CFR 681, Appendix A to Part 681, is available as an online resource).

**Red Flags Suggested by the FTC**

*Alerts, Notifications, or Warnings from a Consumer Reporting Agency*

- A fraud alert (“initial fraud alert” for 90 days or “extended fraud alert” for up to 7 years) 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, as defined by 16 CFR 641.1(b). (NOTE: Receipt of such notice requires a written response from the dealer. See the Address Discrepancy Form & Instructions and the Address Discrepancy Rule 16 CFR 641.1 available as online resources.)
- 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 recent and significant increase in the volume of inquiries;
  - An unusual number of recently established credit relationships;
  - A material change in the use of credit, especially with respect to recently established credit relationships; or
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

*Suspicious Documents*

- 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.
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.

An application appears to have been altered, forged, or gives the appearance of having been destroyed and reassembled.

**Suspicious Personal Identifying Information**

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - The address does not match any address in the consumer report; or
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.
- 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.
- 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:
  - The address on an application is the same as the address provided on a fraudulent application; or
  - The phone number on an application is the same as the number provided on a fraudulent application.
- 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:
  - The address on an application is fictitious, a mail drop, or a prison; or
  - The phone number is invalid or is associated with a pager or answering service.
The SSN provided is the same as that submitted by other persons opening an account or other customers.

The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.

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 is not consistent with personal identifying information that is on file with the financial institution or creditor.

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.

**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**

- 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.

**Factors to Consider in Identifying Dealership-Specific Red Flags**

In identifying Red Flags that apply to your specific dealership operations, it’s helpful to draw on real-world scenarios specific to automobile retail sales and consumer lease transactions as sources. Obviously, your dealership’s actual identity theft experiences should also be weighed.

In some cases, a customer’s behavior or efforts to finalize a deal that fall out of the norm of typical dealership transactions can raise a Red Flag. These are called “Anomaly Deals.”

**Anomaly Deals**

- **PHANTOM BUYERS**
  Transactions where all or key portions of the sales and funding processes are conducted by phone, fax, or the internet. Situations where the customer in the dealership is acting on someone else’s behalf (regardless of the reason given—actual customer ill, incapacitated, out of town, etc.). Deals where delivery is to be made at a location outside the dealership where the phantom buyer is located.

- **FRENETIC DEALS**
  Situations where the customer asserts that the deal must be consummated in a timeframe that is considerably shorter than what is logically required to properly select, negotiate, document, and fund a vehicle purchase. Attempts by the customer to skip or postpone key aspects of the transaction due to unusually tight time constraints.

- **CALAMITY CUSTOMERS**
  Transactions where the customer claims to be the victim of a calamity that requires a major deviation from normal buying and funding practices (“As a hurricane victim, I still don’t have a permanent address”, “I lost my Social Security card in a fire”, etc.) Situations when sympathy or the need to come to the customer’s aid is a driving force in deviating from established policies or quickly consummating the deal.
- **JACK-AND-THE-BEAN-STALK DEALS**
  Transactions where the customer is attempting to trade a current or recent low-mileage vehicle for a similar new or used vehicle for no apparent reason. Situations when the customer, as an expressed means of facilitating a quick approval, is nonchalant as to the price of the vehicle, trade allowance, monthly payment, term, APR, etc.

- **AIR DEALS**
  A situation where the customer is attempting to structure the deal or arrange for funding when they have little or no real money or equity in the purchase. The customer can only make a token down payment, it must be charged to a credit card, the customer wants to make a deferred down payment (in California), a hold check or pick-up payment, or the customer has little or no equity in the vehicle being traded in, or the trade-in is worthless.

**Customer Risk Levels**
While every customer should be scrutinized, logic dictates that some require more attention than others. The odds of a repeat buyer – who can provide all of the required information and who is buying the car in person – trying to use someone else’s credit are between slim and none (though proper precautions should always be taken). However, a first-time internet buyer who has never set foot in the dealership warrants additional scrutiny (especially if the data entered on the credit application contains discrepancies such as address or employment history). In order to reduce the time required to manage the program and ensure that resources are directed to those situations in which Red Flags are more prone to occur, dealership customers may be assigned to one of three risk categories.

**Green Flag Customers**
Customers who:
- are known personally by someone in the dealership for a period of two or more years via community connections – school, church, business, professional or fraternal organizations, etc.;
- are employed for a period of time greater than two years;
- are second- or multiple-time buyers;
- are conducting the purchase in person; and
- pass the F&I DeskCheck*

**Blue Flag Customers**
First time customers who:
- pass the F&I DeskCheck* and
- are conducting the transaction in person.
Red Flag Customers

Any customer who:

- cannot provide all of the necessary background information;
- cannot provide a photo ID (driver's license);
- provides one or more addresses that cannot be tracked or tied to the other information provided or reasonably verified;
- is conducting all or a portion of the transaction via the phone, fax, or internet;
- does not pass the F&I DeskCheck*; or
- triggers a warning, notification, or alert from a reporting agency or protection service.

*Developed by Member Benefits Services, Inc. for F&I practitioners, the F&I DeskCheck is a tool that provides a quick and consistent method of verifying the accuracy of information provided by customers. A detailed explanation is provided later in this section.

Other Suggested Dealership Red Flags

- The customer fails to pass the F&I DeskCheck.
- Anomaly deals.
- If a challenge question (explained below) is used, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- Warnings, notifications, or alerts received from consumer reporting agencies (credit bureaus) or fraud detection services.
- The dealership is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that a fraudulent account has been opened for a person engaged in identity theft.
- Indicators based on the dealership’s actual experience with identity theft. If a dealership has encountered identity theft in the course of doing business (either a transaction in which identity theft occurred or was attempted) and an indicator of that identity theft (a clue that the customer was not who they claimed to be) is not included in the Red Flags listed above, then that specific indicator should be identified and added to the dealership’s ITPP.
- Any FTC-suggested Red Flags not incorporated into the list above deemed to be applicable to the dealership.

Detecting Red Flags

Since information collection and authentication is vital in detecting Red Flags, a crucial component of any ITPP is the F&I DeskCheck, a verification process proposed by Member Benefits Service, Inc. that uses data triangulation methodology. The DeskCheck serves two purposes. First, it ensures that every customer is subjected to a documented identity check using the same criteria, and second, it’s an efficient tool for quickly determining whether additional scrutiny is warranted. (A laminated copy of the F&I DeskCheck is included in your Nonpublic Personal Information (NPI) Compliance Binder)
F&I DeskCheck
The F&I DeskCheck provides a checklist for verifying the authenticity of a customer’s information. To complete the F&I DeskCheck:

1. Secure a photocopy of the customer’s driver’s license.
2. Record or cause to be recorded responses to all credit application inquiries regarding personal information, employment history, and credit information for a period of not less than five years. A customer making the purchase in person must sign the form; an online customer must grant permission for a credit report to be secured and provide a means of confirming his or her identify through challenge questions.
3. At an appropriate point in the purchase/funding process, secure a photocopy of the customer’s insurance verification card.
4. Inspect the driver’s license and insurance verification card to determine whether they are valid, up-to-date, original, unaltered, authentic documents and whether the picture on the driver’s license appears to be a photo of the customer.
5. When appropriate, obtain a copy of the customer’s credit report.
6. Conduct a residence address and employment triangulation with the information at hand.

A triangulation is simply verifying that the information matches on at least three different documents. Note any discrepancies between the various documents and only ask the customer to clarify as needed. The triangulation should include the driver’s license, insurance verification card, credit application, and credit report (each when appropriate).

For example, the home address on the customer’s driver’s license is different from those listed on the application and credit report. However, the employment information on both the application and credit report show a job change that involved relocation from another part of the state, which coincides with the listed previous and current residence address locations and dates. In this case, the customer simply has not taken the steps to update his driver’s license. The information must still be reasonably verified and documented, but unless the customer is unable to do that, it is not yet a Red Flag.

If the information and the explanations do not seem likely and cannot be verified, then the Customer Contact Representative is to report their findings to a Red Flag Coordinator.

7. If necessary, conduct a verification of the Social Security Number (beyond checking it against the number listed on the credit report). It should be checked against the Social Security Administration’s Death Master List and the state of issue should be verified (as indicated by the first three numbers). Some dealerships may have additional software or processes.

Whether and when the heightened Social Security Number check comes into play should be specified in the dealership’s ITPP. This step may be optional for green flag customers – and possibly blue flag customers, depending on the situation.

If key customer information cannot be provided or is out of sync with information from other sources, the customer’s explanations are convoluted, or the individual qualifies as a Red Flag customer, the in-depth Social Security Number check should be conducted before reporting the findings to the Red Flag Coordinator.

If the F&I DeskCheck does not show any Red Flags or if the Red Flags are cleared, the Customer Contact Representative should make a notation on the credit application – initials followed by the date and a check. The F&I practitioner can use one of the F&I DeskCheck
stickers included with the binder and available as an online resource.

Using Challenge Questions
Challenge questions ask a buyer to recall information to a personal question in an attempt to confirm their identity (e.g., mother’s maiden name, former employers or former home addresses, dollar amount of remaining mortgage, etc.). Special care should be taken when using challenge questions to use out-of-wallet information (information not readily available if the buyer is an identity thief in possession of a stolen wallet – see below). The F&I manager employing this device should choose a question to which he or she knows the answer as a result of a document obtained by dealership with the buyer’s information (e.g., credit history report) and not information provided by the buyer (e.g., credit application).

- **In-Wallet Information** – Information that could be found in someone’s wallet (driver’s license number, home address, place of employment, etc.)
- **Out-of-Wallet Information** – Information that is unlikely to be found in someone’s wallet (former home addresses, former places of employment, remaining dollar amount of existing mortgage, etc.)

One easy way to use challenge questions is to point out information that is not true. For example, if the credit history report shows that the customer lived in Akron, Ohio, in the early 80s, you might note to the customer that you see they lived in Cincinnati. A legitimate customer will correct you. Consult your legal counsel or Corporate Compliance Officer for more information about your dealership’s policies on the use of challenge questions.

Responding to Red Flags
The Red Flags Rule requires creditors to develop responses to Red Flags as part of their ITPP. The FTC suggests that creditors consider the following responses to Red Flags in developing their program, with the understanding that not all will be applicable to all creditors.

Responses to Red Flags Suggested by the FTC

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

Other Suggested Responses to Red Flags

Under the Red Flags Rule program proposed in this guide, the Red Flag Coordinator, after being alerted to a Red Flag by the Customer Contact Representative, will review all the information provided by the customer and other sources to determine the best course of action. The most common initial response will be to direct the F&I practitioner to secure additional information,
obtain a clarification, or conduct a Social Security Number verification.

If the situation dictates, the Red Flag Coordinator may deal directly with the customer and consult with the Corporate Compliance Officer. A decision must be made about whether the deal can proceed and whether regulatory or law enforcement officials should be notified. In no case should a vehicle be spot delivered or the transaction consummated with an open or unresolved Red Flag. It is helpful to identify the contact name, department, and phone number of the official you need to contact in the ITPP hierarchy so it is available for quick reference if you need it.

**Updating and Documenting the Program**

The FTC requires creditors to update the program (including the Red Flags determined to be relevant) periodically to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft, based on factors such as:

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

The Corporate Compliance Officer is responsible for documenting and updating the program. The documentation will include:

- The written ITPP as approved by the board;
- Copies of credit applications marked with initials and date to note completion of the F&I DeskCheck;
- Incident reports (prepared by the Red Flag Coordinator or Corporate Compliance Officer); and
- Periodic reports, at least annually (prepared by the Corporate Compliance Officer).

**Oversight of Service Providers**

If the dealership chooses to use an outside Service Provider for customer identity verification or other Red Flags Rule-related tasks, the Corporate Compliance Officer will be responsible for overseeing the service provider relationship. The dealership could also require other Service Providers by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the Service Provider's activities and either report to the dealership or take appropriate steps to prevent or mitigate identity theft. Service Providers would be responsible to the dealership as outlined in the Service Provider ITPP Agreements available as online resources.

*Any third-party agreement should be thoroughly reviewed by counsel and included as part of the dealership’s ITPP.*

**Filing Suspicious Activity Reports**

According to 31 U.S.C. 5312(a)(2)(T), automobile dealerships are subject to 31 U.S.C. 5318(g),
which requires financial institutions and creditors to file a suspicious activity report (SAR) in accordance with applicable law and regulation to report any suspicious financial transaction relevant to a possible violation of law or regulation. The SAR is filed electronically with the Financial Crimes Enforcement Network (FinCEN), an agency of the United States Department of the Treasury. You may file a SAR with FinCEN at www.fincen.gov/forms/bsa_forms. The goal of SAR filings is to help the Federal government identify individuals, groups, and organizations involved in fraud, terrorist financing, money laundering, and other crimes.

The Corporate Compliance Officer is responsible for determining whether a SAR should be filed and for preparing and filing the report. Not every unresolved Red Flag will require that a SAR be filed. Common sense – and consultation with the dealer principal and / or corporate counsel – will help determine the proper course of action.

No documentation is to be submitted with the SAR, but the dealership should collect all supporting documentation and retain it for the required record retention period. The regulation states that the customer is not to be notified that a report has been filed. Instructions for electronically filing a SAR with FinCEN through the BSA E-filing system are located at www.fincen.gov/forms/files/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf.

**Responding to Notices of Address Discrepancy**

If the dealership receives a notice of address discrepancy from a credit reporting agency in conjunction with a credit history report, the F&I practitioner is responsible for sending an Address Discrepancy Form to that agency if the F&I practitioner is able to reasonably verify the customer’s identity and form a belief that the address provided by the customer is correct. The Address Discrepancy Rule section 16 CFR 641.1, an Address Discrepancy Form, and Instructions are available as online resources.
ITPP General Procedures

1. A DeskCheck (basic review of all pertinent information) will be conducted for all applicable transactions (credit-related transactions, lease transactions and parts and service transactions), with a designating sticker or other suitable identifying mark (initialed and dated) affixed to the credit application (or related documents) indicating that Buyer information verification has been completed and either no Red Flags were identified or all identified Red Flags have been cleared.

2. If Dealer receives a notice of address discrepancy from a credit-reporting agency in conjunction with a credit report, the Red Flags Coordinator will complete and submit an address discrepancy notice to the agency if he or she can reasonably verify Buyer’s identity and resolve the address discrepancy.

3. If a Red Flag is identified in any potential transaction, the Customer Contact Representative is to consult with the Red Flags Coordinator for guidance on how to proceed.

4. The Red Flags Coordinator will review all of the relevant information. In some cases, the Customer Contact Representative will be asked to gather more information or secure a clarification. In other situations, the Red Flags Coordinator will meet with Buyer. Also, the Red Flags Coordinator may consult with legal counsel or the Corporate Compliance Officer for guidance.

5. The Red Flags Coordinator must complete and file an Incident Report (with supporting documentation) in the ITPP file within 24 hours of an attempted or actual identity theft.

6. The Corporate Compliance Officer will respond to notices from credit reporting agencies, funding sources or other Service Providers, Buyers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts originated by Dealer; contact the appropriate authorities in cases of suspected, attempted, or actual identity theft; and file the Suspicious Activity Report (SAR), if applicable.

7. As needed, the Corporate Compliance Officer will review Incident Reports and evaluate the ITPP’s efficacy.

8. The Corporate Compliance Officer will prepare the ITPP Periodic or Annual Report and submit them for Board approval. ITPP updates or revisions applicable to the period are to be included in this report. The report should: 1) evaluate how effective the program has been in addressing the risk of identity theft; 2) indicate how the practices of the service providers are monitored and their effectiveness; 3) list any incidents of identity theft and the response; and 4) make any recommendations for changes to the program.

9. The Board will review the Periodic or Annual Reports timely.
ITPP Operational Procedures

The following procedures will be followed by Dealer employees or responsible parties in the course of applying the ITPP to daily situations.

Minimum Identification Standards

- A photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) must be presented in the course of any credit-related sale (credit card, solicited in-house finance, or broker or third-party arranged financing), lease transaction, or parts or service transaction. A photocopy of the Driver’s License or submitted ID (front and back) shall be retained by Dealer.

- A photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) must be presented in the course of any Unit being released to someone other than Buyer after the sale or service. A copy of a properly executed Vehicle Release Authorization Form (provided as an online resource) or other suitable third-party release documentation signed by a verified legal representative of Buyer and the designated individual taking possession of Unit, is to be retained by Dealer.

- It will constitute a Red Flag under this ITPP if either Buyer or an individual designated by Buyer to take possession of the Unit (at a time or location other than when or where the sale was consummated) is unable to produce a photo-bearing Driver’s License or photo-bearing government-issued form of identification or if there is evidence of that identification being altered, invalid, or having the incorrect address or if an individual designated by Buyer to take possession of the Unit (regardless of when or where that individual takes possession) is unable to produce a properly executed Vehicle Release Authorization Form or other suitable third-party release documentation.

Credit Card Sales – Minimum Information Collection Standards

- Credit card sales with a total charge in excess of $500 for any item or service require the presentation of a photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) for review by Dealer employee and comparison to the credit card to be used for the transaction.

- Credit card sales in which all or a portion of the purchase price of a Unit or service of any type require the presentation of a photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) for review by Dealer employee. A photocopy of the Driver’s License or submitted ID (front and back) shall be retained by Dealer.

- It will constitute a Red Flag under this ITPP if either a Buyer or an employee or agent of the Buyer (who is charged with making the purchase and/or taking possession of the Unit) is unable to produce a photo-bearing Driver’s License or photo-bearing government-issued form of identification or if it is determined that the identification offered has been altered, is invalid, or does not reflect a current address.
Brokered or Otherwise Arranged Third-Party Financing – Minimum Customer Information Collection Standards

Brokered or otherwise arranged third-party financing arrangements are instances in which Dealer is not listed as the creditor on the installment sales agreement. Dealer may collect and forward the credit application and related purchase documents to the broker or other third-party. Credit terms negotiations; document verifications; the securing of credit history reports; and the acceptance or rejection of the requests for credit, credit document preparation, and Contract disclosures are handled by the broker or third party referred to in the ITPP as a Service Provider. If approved, either a check payable to Dealer is given to the Buyer or sent to Dealer. Dealer takes no other active interest other than (if applicable) completing the credit application or directing the Buyer to prospective credit source(s).

- A photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) must be presented in the course of any Unit being funded by sources recommended or arranged by Dealer. Two photocopies (front and back) of the Driver’s License or other acceptable ID are to be prepared, with one retained by Dealer and the second forwarded in the packet sent to the Service Provider or (if policy so dictates) included with the credit request material (credit application) submitted to the Service Provider(s).

- (If applicable) Prepare or cause to be prepared a fully completed and signed credit application by Buyer. Capturing all of the requested information on an application is a requirement of this ITPP.

- A copy of a Service Provider ITPP Agreement is to be transmitted to and signed by each Service Provider and returned to Dealer for inclusion in the NPI Compliance Binder. (The Agreement must indicate exactly which information collection and credit application completion processes are to be undertaken by Dealer, under the aforementioned circumstances that fall within the purview of the ITPP.)

In-House Funding Solicitation, Negotiation, Documentation, and Contract Disclosures – Minimum Information Collection Standards

Funding solicitation, negotiation, documentation, and Contract disclosures that are conducted in-house by Dealer under wholesale agreements with Service Providers are instances in which Dealer is listed as the creditor on the Contract, with the Contract assigned to the approving Service Provider.

Dealer collects and forwards the credit information and related purchase documents to its relevant Service Providers. Term negotiations, DeskChecks, document preparation, and Contract disclosure and signature collection is handled by Dealer in consultation with the Service Providers.
- A photo-bearing Driver’s License or photo-bearing government-issued form of identification (affirmed to be non-altered, valid, with a current address) must be presented in the course of any Unit being leased or funded through Service Providers recommended or arranged by Dealer. Two photocopies of the Driver’s License (front and back) are to be prepared, with one retained by Dealer and the second forwarded in the packet sent to the Service Provider or (if policy so dictates) included with the credit request material (e.g., credit application) submitted to the Service Provider(s).

- Prepare or cause to be prepared a fully completed and signed credit application. Capturing all of the requested information on an application is required by this ITPP.

- (As required) Secure a copy of Buyer’s insurance card. Photocopy twice, once for Dealer and once to be sent to the prospective Service Provider(s).

- As per Dealer policy, submit the credit application to a credit-reporting agency to secure a copy of Buyer’s credit history report.

- Compare the address and other pertinent information between the Buyer’s or Purchase Order, credit application, and credit agency to ensure they match. Any material discrepancy constitutes a Red Flag under this ITPP. (One copy of a standard Red Flag F&I DeskCheck comes with your DealerAide: Nonpublic Personal Information Compliance Program. You may order additional copies for additional employees or create your own custom DeskCheck as necessary. Once the DeskCheck you choose to use has been approved by competent corporate counsel, a copy should be placed in the “Resources” section of your binder.)

- Weigh the information provided by Buyer and generated by the credit-reporting agency against the other possible applicable Red Flags described in the ITPP. Any inconsistency constitutes a Red Flag under this ITPP.

- In the cases in which the individual Service Provider is responsible for identifying Red Flags, the respective duties and standards of both Dealer and the Service Provider are to be identified in writing in a Service Provider ITPP Agreement or similar document.

- In the event no Red Flags have been detected, a DeskCheck sticker or other suitable identifying mark should be affixed to the copy of the credit application or similar document retained by Dealer to affirm that a check has been completed. This is an ITPP requirement.

- It is a requirement of this ITPP that one or more individuals assigned to processing the deals be tasked with affirming that an initialed and dated DeskCheck sticker (or suitable identifying mark) is affixed to every credit application or similar document processed by Dealer. A deal cannot be closed if the credit application or similar document does not contain an initialed and dated DeskCheck sticker or other designating mark.
Investigating & Clearing Red Flags

The following standards for investigating and clearing Red Flags – whether the Red Flag was identified by an outside source or an in-store employee – are required by Dealer ITPP.

- When a Red Flag is detected, the Customer Contact Representative, without alerting the Buyer of the discrepancy, will contact the on-duty Red Flags Coordinator (or the Corporate Compliance Officer if the Red Flags Coordinator is unavailable) for advice on how to proceed. In cases in which a Red Flags Coordinator or the Corporate Compliance Officer are assisting other Customer Contact Representatives or are otherwise unavailable, the Customer Contact Rep may continue processing the transaction until they are available, but a deal may not be consummated and a vehicle may not be spot delivered until the Red Flag has been cleared.

- The individual tasked with reviewing Red Flags (i.e., the Red Flags Coordinator) will employ the following procedures to confirm that a Red Flag actually exists: Conduct a review of all relevant information to confirm the presence of a Red Flag as identified or defined by the ITPP. Depending on the situation, either intercede or direct others to secure from Buyer additional documentation to clear the discrepancy, conduct a Social Security Number state of issue verification or deceased person’s verification, contact current and former employers, landlords, next of kin, or other sources listed on the credit application or listed on the credit history report, enlist the help of the lending sources weighing the merits of the transaction, respond as required to fraud alerts and credit freezes, and take the other steps authorized by the ITPP.

- If the Red Flag can be cleared, the deal can proceed to consummation. If the Red Flag was reported by a third-party source (i.e., Service Provider), the fact that Red Flag was cleared must be communicated to the reporting source.

- If the Red Flag cannot be cleared, the events that precipitated it must be documented in an Incident Report, with the required supporting material included therein and filed in the ITPP file. If applicable, the proper authorities as detailed below are to be notified.

Police Phone Number:
Contact Name:

(It is recommended that a specific contact be identified with the corresponding phone number. In most cases, an emergency call to 911 is unnecessary and beyond the scope of the assistance required.)

- Under no circumstances is a Unit to be delivered or the paperwork consummated if an open Red Flag cannot be cleared.

- Buyer should not be alerted (or confronted) if a Red Flag cannot be cleared.

Employee Awareness Training & Specific Task Assignment and Training

Affected employees must be trained to implement the ITPP. ITPP training is an important element of compliance with the Red Flags Rule. The following training standards are required by Dealer
ITPP.

- Employee training (extended to all current employees) based on Dealer ITPP will be completed by the ITPP implementation date. The Corporate Compliance Officer is responsible for assigning ITPP tasks and developing and conducting the training sessions or locating a qualified third-party resource to do so. Each employee will complete a Job Description Affirmation Form, which is to be maintained in the NPI Compliance Binder.

- New or reassigned employees who have designated duties under Dealer ITPP will be properly trained. They will complete and sign a Job Description Affirmation Form a copy of which is to be filed in the NPI Compliance Binder with a copy given to the employee and original placed in their personnel file.

- Employee training will be conducted periodically to ensure all employees are aware of changes to the ITPP or new trends in Identity Theft in general. These training sessions should occur at least as often as there are changes to the ITPP. Additionally, all employees will receive emergency training when an attempted or actual identity theft occurs.

- All training and retraining will be documented in writing each time new or retraining occurs.

**Incident & Annual Reports**

- **Incident Reports:** The Corporate Compliance Officer will compile (with supporting documents) a written report documenting an attempted Identity Theft (a Red Flag that could not be cleared, resulting in the sale not being consummated) or actual theft within 48 hours of the event. The report will be included in the ITPP file. A summation of all Incident Reports for the preceding twelve months (or all months since the last report was filed) will be included in the ITPP Periodic or Annual Report.

- **Periodic or Annual Reports:** The Corporate Compliance Officer will timely compile and complete for Board approval the ITPP Periodic or Annual Report.
ITPP Owner’s Manual

This Section of the handbook is your ITPP Owner’s Manual. It contains the information necessary to actually perform the tasks you have been assigned in accordance with Dealer’s ITPP. It will aid you in the application of the requisites imposed by the ITPP on a daily basis and is offered as a best-practices resource. THIS IS NOT OPTIONAL READING; YOU WILL BE HELD RESPONSIBLE FOR THE MATERIAL IN THIS SECTION. THE INFORMATION CONTAINED IN THIS SECTION IS ESSENTIAL FOR FEDERAL RED FLAGS RULE COMPLIANCE. ITPP procedures implemented by your store should be clearly outlined and made available to all employees.

General Procedures (All Employees)

Write things down. Compliance with FTC regulations means that you must properly document transactions, keep copies of relevant forms, and provide a written narrative of the events. When applicable, document your exchanges with the Buyer in the course of collecting and clarifying ITPP-based information. Write down phone numbers, names and statements made by the Buyer. Do not attempt to rely on your memory when asked to recount the events to a Red Flags Coordinator, Corporate Compliance Officer, or in worst-case scenarios, to law enforcement officials or a court of law.

A Red Flag does not, in and of itself, indicate illegal or nefarious activity. A Red Flag simply indicates that information must be clarified and documented. Failure to detect or clear a Red Flag creates an opportunity for Identity Theft to occur. Most Red Flags will clear upon further inspection, so it is important to avoid treating any Buyer like a criminal.

* * *

Performing a Basic DeskCheck (Customer Contact Representative)

The Customer Contact Representative must complete a basic DeskCheck on each and every deal. Refer to any word tracks provided by your dealer for guidance on keeping the information collection and clarification process Buyer-friendly. A DeskCheck requires that the Customer Contact Representative complete the following six steps:

Responses must be recorded to all credit application inquiries for personal information, employment history and credit information for a period of not less than the past five years. An in-person Buyer must sign the form; an online Buyer must grant permission for a credit history report to be secured and provide a means of confirming his or her identity (an online Buyer can confirm his identity by answering questions only the Buyer would know, for example, the outstanding balance on their mortgage, etc.). This is an ITPP requirement.

Secure a photocopy of the Buyer’s Driver’s License as per ITPP minimum standards. Note that a Buyer with an expired Driver’s License would not pass the DeskCheck.

Secure a photocopy of the Buyer’s insurance verification card. When the insurance card is collected is a matter of Dealer policy. Proof of insurance card(s) may or may not be collected and copied when the credit information is collected. However, best practices dictate that the proof of insurance cards be collected at the time the credit application is completed.

Inspect the Driver’s License and insurance verification card to determine whether they are valid, up-to-date, original, unaltered, authentic documents, and whether the picture on the Driver’s License appears to be a photo of the Buyer.
Obtain a copy of the Buyer’s credit history report. If there are freezes, alerts or warnings on the Buyer’s credit history, then the Customer Contact Representative should assist the Buyer in lifting them by providing access to the phone number and by allowing the customer to make contact while in the store. Also, the customer should be allowed to provide the PIN or other identifying information in private.

Conduct residence address and employment history verification.

Compare the residence address on the Driver’s License, insurance verification card, credit application, and credit history report to ensure they are consistent.

Compare the employment history on the credit application to the credit history report to ensure they are consistent.

Make note of any discrepancies between the various documents and ask the Buyer to clarify and supply documentation as needed.

(For example, the home address on the Buyer’s Driver’s License is different from those listed on the application and credit report. However, the employment information on both the application and credit report show a job change that involved relocation from another part of the state, which coincides with the listed previous and current residence address locations and dates. In this case, it is possible the Buyer simply hasn’t taken the steps to update his license. Obtain and file official documentation of the relocation.)

Verify the authenticity of the Buyer’s Social Security Number.

**State of Issue Confirmation** – Use the chart provided by the Social Security Administration (see web address below) or on the back of the Red Flag F&I DeskCheck card that came with the DealerAide: Nonpublic Personal Information Compliance Program to check the first three digits of the customer’s Social Security Number to determine the state of issue and verify that it is consistent with the customer’s declared state of issue. Please note that the chart is a guide, and is not necessarily definitive proof of the customer’s identity. See any word tracks provided by Dealer for guidance.

Social Security State of Issue Chart
http://www.socialsecurity.gov/employer/stateweb.htm

**Death Records Confirmation** – Check the Social Security Administration’s Death Master File at stevemorse.org/ssdi/ssdi.html and select FamilySearch as the search engine.

**Identity Verification Confirmation** – (Optional) Use a Social Security Number verification service from a Service Provider (please note these records are not necessarily as accurate as those available from the SSA or IRS). Please see www.ssa.gov and the individual company’s Terms of Service for specific restrictions for use.

**Transactions Being Conducted Via the Internet or Fax**

If Dealer has a reasonably compliant mechanism in place for conducting internet or fax transactions without the Buyer entering the store, follow the guidelines provided by Dealer.

If a reasonably compliant mechanism is not in place for online transactions or transactions via fax and the Buyer has not come to the store in person at any point in the process, then the Buyer should be informed that the deal cannot proceed unless he or she comes to the store in person. If the Buyer declines the request, the case should be turned over to the Red Flags Coordinator, who will make a judgment regarding whether to terminate the deal and/or contact...
If the Buyer arrives at the store, secure a photocopy of the Buyer’s Driver’s License and compare the likeness in the photo on the Driver’s License to the Buyer who presented it and verify that the license has not been altered. Perform any additional DeskCheck steps that were not previously completed. Then the Buyer must sign the credit application.

* * *

**Addressing Credit Warnings,**

(Customer Contact Representative

**Fraud Alerts, Active Duty Alerts, and Credit Freezes** and/or Red Flags Coordinator)

NOTICE: If the Buyer’s credit history contains a credit warning, fraud alert, or credit freeze, the transaction cannot proceed until all such warnings, alerts, or freezes have been addressed.

**Credit Warnings, Fraud Alerts, Active Duty Alerts, and Credit Freezes**

Remember that only the Buyer (or a designate in the case of an Active Duty Alert) can initiate the action required to implement an alert or freeze with a credit bureau. If a Buyer expresses a lack of knowledge of the alert or freeze, this should constitute a Red Flag and you should proceed with caution.

If you are notified that an alert or freeze has been placed on an account, inform the Buyer that he or she must lift the alert or freeze (at least temporarily) for the deal to proceed. You may provide the Buyer the credit bureau’s instructions on lifting the alert or freeze which are provided as an online resource. All of the documentation the Buyer requires to lift the alert or freeze was provided to him or her by the credit bureau with which they placed the alert or freeze.

Once the file has been unlocked or unfrozen, if a captive or institutional lender ran the credit report, advise them of what has transpired and ask them to process the request a second time.

Do not proceed with the transaction if the Buyer cannot unlock the file within a reasonable length of time. Bear in mind, it may take as much as 30 minutes for the request to be processed and access allowed. The deal should be put on hold and subjected to further scrutiny by the Red Flags Coordinator if the Buyer must leave the Dealership (for any reason).

Because an alert or freeze is most often initiated by the Buyer as the result of an attempted, anticipated, or actual identity theft, the Buyer should understand the delays for removing the lock on their credit information.
**Other Alerts or Warnings**
If you are notified by a Service Provider or other authorities that an alert or warning is associated with the Buyer, do not inform the Buyer. You will require assistance from the Red Flags Coordinator who will make a determination on how to proceed.

**If an alert, freeze, or warning cannot be lifted or cleared with the tools and options available to the Customer Contact Representative, this constitutes a Red Flag – contact the Red Flags Coordinator.**

* * *

**Clarifying Potential Red Flags**

*The Customer Contact Representative should make the Buyer aware of missing or discrepant information. If after being notified of the issue, the Buyer is unable to provide or clarify the information, the Red Flags Coordinator will take over.*

In the event that one or more potential Red Flags arise during the basic DeskCheck, you must take steps to resolve each Red Flag and document the reasons for the inconsistencies. The most common hurdles you'll likely encounter in completing the DeskCheck are incomplete Buyer information and discrepancies in the information provided by the Buyer and other sources. Word tracks may be provided by Dealer.

**Missing information – Credit Applications**

If information is missing from a credit application, please instruct the Buyer to provide the missing details. Because the Buyer is required to recall details that may be several years old, he or she may need to take additional steps to acquire it (look up an old rental agreement, etc.). This alone does not constitute a Red Flag. The Buyer should be allowed to take reasonable steps to obtain the information.

However, it's important that you maintain control of the situation. If the Buyer needs to make a call (even if it’s long distance), make your phone available, and unless the item is highly personal, stay in the room. When possible, secure related information or a phone number and make the call yourself (which, if possible, you should do out of the presence of the Buyer). If the Buyer intends to perpetrate a fraud, any corroborating information you ask the Buyer to provide may be fraudulent, obfuscated, or misleading.

In some cases, the Buyer may fail to see the importance of providing credit information. Depending on the situation, the Customer Contact Representative may wish to inform the Buyer that the deal cannot proceed without the missing information (see word tracks provided by Dealer) or bring in a Red Flags Coordinator to explain the issue. Faced with the prospect of not getting the deal done, most legitimate Buyers will put forth the effort to provide the missing information, especially if the request is framed in a friendly, non-adversarial manner.

Please note that you cannot tell a Buyer the Red Flags Rule requires that he or she provide all of the information requested on the credit application because the Rule does not make a specific reference of this type. You can tell them that Dealer is committed to fighting Identity Theft and it is Dealer’s policy that all credit applications be complete.

It is a requirement of this ITPP that you have a fully completed and signed credit application.
Missing Information – Driver’s Licenses
All applicants for credit must present a valid Driver’s License or photo-bearing government-issued identification, even if they’re not the primary Buyer of the Unit.

The Driver’s Licenses of those completing credit applications should be collected and photocopied.

It is permissible to ask the Buyer Challenge Questions in an attempt to confirm the information being presented is attributable to the Buyer divulging it. However, pursuant to Dealer ITPP, you must treat the Buyer with respect – do not be confrontational or accusatory.

If the Customer Contact Representative cannot collect all of the required information, this constitutes a Red Flag – contact the Red Flags Coordinator. The Red Flags Coordinator must take additional steps to clarify the information or determine that the Red Flag cannot be cleared and contact the Corporate Compliance Officer to terminate the transaction. The Red Flags Coordinator must complete an Incident Report. If recommended by your corporate counsel, the Corporate Compliance Officer must complete and submit a SAR.

Information Discrepancies – Credit Applications
In the case of inconsistencies between the credit application, the credit report and documentation supplied by the Buyer, you should ask the Buyer to explain (and provide documentation of) the reason for the discrepancies. In many cases, it is best if you make the verification yourself, rather than rely on the Buyer. If the Buyer intends to perpetrate a fraud, then the substantiating information you ask them to provide may be fraudulent, obfuscated, or misleading.

(For example, the current employer recorded on a credit application does not match the current employer listed on the credit report. The Buyer indicates that the employer listed on the credit application is a new one. If possible, ask the Buyer who their direct supervisor is at their new place of employment, look up the number of that company online or in the phonebook, and use the phone number listed there to call and confirm with the current supervisor or HR department that the Buyer is an employee. Ask for a physical description of the employee if it would be known by the individual you contact. Obtain and file documentation of the resolution to this discrepancy.)

Note that the failure to list a leisure residence on a credit application or to have a landline doesn’t necessarily indicate an illegal activity.

Information Discrepancies – Driver’s Licenses
It is recommended that if the Driver’s License offered for photocopying does not belong to the individual who signed the credit application, the transaction be put on hold pending further investigation by the Red Flags Coordinator. Buyers will offer a host of often legitimate reasons (e.g., left ID at home), but truthful or not, the Driver’s License you inspect and document for the transaction must match the identity of the individual completing the credit application.

In other situations, a third party may be attempting to purchase a Unit for someone who is unable to be present (e.g., in the hospital, overseas). Even if the third party has the Driver’s License of the individual for whom they claim to be purchasing (and complete the credit application in that person’s name), do not proceed under any circumstances until the actual buyer – also subjected to Red Flags Rule verifications – has communicated to the Customer Contact Representative or other ITPP official his or her approval (supported by an affirming document such as a vehicle purchase-specific notarized power of attorney, corporate resolution, or other legally binding written authorization).
If the Customer Contact Representative cannot clarify all discrepancies, this constitutes a Red Flag – contact the Red Flags Coordinator. The Red Flags Coordinator must take additional steps to clarify the information or determine that the Red Flag cannot be cleared and contact the Corporate Compliance Officer to terminate the transaction, complete an Incident report, and determine whether or not to contact authorities. The Red Flags Coordinator must complete an Incident Report. If recommended by your corporate counsel, the Corporate Compliance Officer must complete and submit a SAR.

Possibly Fraudulent Documentation – Driver’s Licenses
In cases in which the Driver’s License appears to have been altered or the photo does not appear to match, the deal should not be consummated until the Driver’s License can be verified. In some states and cases, devices or services are available in-house to confirm Driver’s License information or can be obtained from a Service Provider.

Best practices dictate that unless the transaction is a spot delivery, time is available to verify the Driver’s License before the deal is consummated. If the vehicle will not be delivered immediately, the discrepant information can be affirmed or disaffirmed without the Buyer being informed that the authenticity of the license is in question.

However, if it is a spot delivery, the Unit should not be released until the Driver’s License-related Red Flag is addressed.

If the Driver’s License cannot be authenticated, or for any other reason the Red Flags Coordinator suspects attempted identity theft is in progress, the Corporate Compliance Officer is to contact law enforcement authorities.

If the Driver’s License appears to be altered or the photo may be inconsistent with the physical characteristics of the individual presenting it, this constitutes a Red Flag – contact a Red Flags Coordinator. The Red Flags Coordinator must determine whether the Driver’s License is invalid and if necessary, contact the Corporate Compliance Officer to terminate the transaction and determine whether or not to contact authorities. The Red Flags Coordinator must complete an Incident Report. If recommended by your corporate counsel, the Corporate Compliance Officer must complete and submit a SAR.

Problems with Social Security Number

(If the state-of-issue method of authenticating the Buyer’s Social Security Number is not employed by your dealership, ignore all references to that device in this section.)

If the Buyer refuses to or cannot indicate the state of issue of their Social Security Number, do not push the issue. Do not provide a hint of the state signified by the first three digits on the card.

Best practices suggest that any discrepancy with regard to verifying the Social Security Number of the Buyer should trigger additional steps, such as checking the Social Security Death Index, using a Service Provider’s Social Security Number verification system, and/or other further investigation as necessitated by Dealer ITDP.

If the Social Security Number cannot be verified through state-of-issue verification, Service Provider verification system, or other means, or the Social Security Number appears on the Social Security Death Index; this constitutes a Red Flag – contact a Red Flags Coordinator. The Red Flags Coordinator determines whether an identity theft may
be in progress and may contact the Corporate Compliance Officer to terminate the transaction and determine whether or not to contact authorities. The Red Flags Coordinator must complete an Incident Report. If recommended by your corporate counsel, the Corporate Compliance Officer must complete and submit a SAR.

* * *

**Submitting Address Discrepancy Forms** (Customer Contact Representative and/or Red Flags Coordinator)

File an Address Discrepancy Form (provided as an online resource) to the applicable credit bureau if Dealer received a notice of address discrepancy in conjunction with a credit report and you are able, using reasonable procedures such as the DeskCheck, to verify the Buyer’s identity and current address.

The Red Flags Rule requires credit-reporting agencies to notify Dealer if the address information in a request for a credit report differs from the address the agency has on file for a particular Buyer. Dealer is required to respond to the address discrepancy notice from the agency by submitting the correct current address if Dealer is able to develop a reasonable belief that the Buyer is the person he or she claims to be and believes the current address provided by the Buyer to be correct.

The Dealer is only required to send the Address Discrepancy Form to the credit-reporting agency if it has received a notice of address discrepancy from the agency. The Address Discrepancy Form should be mailed to the credit-reporting agency that provided the address discrepancy notice as part of the information Dealer regularly furnishes for the reporting period in which it establishes a relationship with the consumer. In addition to the sheet of address labels for Experian, Equifax, and TransUnion included with the binder, templates for printing additional Avery labels are provided as an online resource.

The information required to complete the Address Discrepancy Form can be drawn from the entries made on the Buyer’s Order and credit application; the information found on the Buyer’s Driver’s License, insurance verification card and credit history report; the information posted to the installment sale or consumer lease agreement and title and registration documents; and conversations with the Buyer.

* * *

**Responding to Red Flags** (Red Flags Coordinator)

The initial response to all Red Flags will be a thorough review of all the information submitted by the Buyer and other sources. The review may include a consultation with the Customer Contact Representative, the Corporate Compliance Officer, and where indicated, legal counsel. This information review should be conducted prior to a determination as to the proper course of action. Every piece of information must be inspected and compared.

Regardless of how suspicious the situation may appear, all exchanges are to be non-confrontational and non-accusatory. You are working under the assumption that the Buyer is who he or she claims to be – you only need to confirm this fact.

When asking for additional information, volunteer to aid in its acquisition, provide store facilities (phone/internet connection) to acquire it, or work through a logical sequence of events (i.e., walk the Buyer through the areas where the inconsistencies exist).
Care must be taken not to provide too much information, thus allowing an imposter to fashion a plausible scenario to explain away an inconsistency.

In cases in which the Buyer simply cannot 1) offer a logical explanation and documentation as to the discrepancies, 2) supply the necessary affirming information, or 3) offer any direction to acquiring the needed information, the Red Flags Coordinator must take action based on when a scheduled delivery of the vehicle is to take place.

If it is slated for a point in the future, the transaction can proceed because time is available to confirm the information tendered by the Buyer – or for the Buyer to secure the required information. You must make clear to the Buyer what is expected, very specifically, of each party and what will (or will not) transpire if the required information or material isn’t received (see suggested word tracks provided by Dealer). While the transaction can continue, it cannot be consummated until all Red Flags have been cleared.

If it’s a spot delivery, the vehicle should not be released until the identity verification issues are addressed. When the issues are reconciled, the Buyer should be contacted and the delivery consummated.

If a Red Flag cannot be cleared with the tools and options available to the Red Flags Coordinator, an attempted identity theft may be in progress – contact the Corporate Compliance Officer to terminate the transaction and determine whether or not to contact authorities. The Red Flags Coordinator must complete an Incident Report. If recommended by your corporate counsel, the Corporate Compliance Officer must complete and submit a SAR.
If All Red Flags Are Cleared
If and when all Red Flags have been cleared, the Customer Contact Representative should affix a DeskCheck sticker or other suitable identifying mark on the credit application (or related documents) indicating that the DeskCheck has been completed and either no Red Flags were identified or all identified Red Flags have been cleared, then initial and date it.

If All Red Flags Are NOT Cleared
If the Red Flags Coordinator cannot clear all Red Flags, assistance from the Corporate Compliance Officer should be requested. In situations in which the transaction must be immediately terminated (as noted by the ITPP, only the Corporate Compliance Officer is empowered to terminate a transaction or alert law enforcement officials), the Customer Contact Representative will not be directly involved in action at this level.

Please note that the Buyer’s inability to help you clear a Red Flag does not necessarily mean they are a criminal, only that it is possible a crime is taking place. Even if law enforcement officials are contacted, the Buyer should not be treated as a criminal – that is for the courts to decide.

Employees of Dealer should take whatever action is indicated by law enforcement officials from that point forward.

If law enforcement officials request that the Buyer be stalled pending their arrival, no employee of Dealer should inform the Buyer of this fact. Simply proceed with the deal as usual (without consummating it) as slowly as possible until they arrive. No employee of Dealer, under any circumstances, should attempt to hold the Buyer if he or she attempts to leave – simply document as much evidence as possible, including any vehicle license plate numbers you can safely obtain.