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

A DEALER GUIDE TO THE

Driven FTC Red Flags and Address Discrepancy Rules

Table of Contents

SECTION ONE

SECTION TWO

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