Chapter 3

Identifying Red Flags

§ 3:1 Overview
  § 3:1.1 “Identity Theft”
  § 3:1.2 “Red Flag”
§ 3:2 Conducting an Initial Risk Assessment
  § 3:2.1 Practical Considerations
  § 3:2.2 Risk Factors to Consider
  § 3:2.3 Other Sources to Consider
§ 3:3 Categories of Red Flags
§ 3:4 Requirement to Update Risks Based on New Threats

§ 3:1 Overview

Each financial institution or creditor must establish reasonable policies and procedures to identify relevant Red Flags for covered accounts and incorporate those Red Flags into a written Identity Theft Prevention Program.
3: Identifying Red Flags

When developing a written Program, one size does not fit all. The Agencies have warned that companies must tailor their Program to their own specific practices and procedures. Merely applying existing privacy and data security practices—“copying another company’s homework”—will not suffice. A company’s Program must be specifically tailored to the types of identity theft risks its customers are exposed to by virtue of the company’s products or services.

§ 3:1.1 “Identity Theft”

When crafting a Program that is intended to mitigate the risk of identity theft, understanding the scope of the term “identity theft” is important. Identity theft is defined under section __.90(b)(8) of the Red Flag Rules as “a fraud committed or attempted using the identifying information of another person without authority.” By cross-reference to FCRA, the term “identifying information” is defined as:

[A]ny name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

(1) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(3) unique electronic identification number, address, or routing code; or

(4) telecommunication identifying information or access device (as defined in 18 U.S.C. § 1029(e)).

Note that the definition of “identity theft” under the Rules looks at more than just the opening of a new line of credit or a financial account. It also includes the unauthorized use of an existing account.

§ 3:1.2 “Red Flag”

The Rules define a “Red Flag” as “a pattern, practice, or specific activity that indicates the possible existence of identity theft.”

Under the Rules, an Identity Theft Prevention Program must reflect the size and complexity of the financial institution or creditor, and the nature and scope of its activities; thus the Red Flags incorporated into a Program must be derived from those very same factors. More specifically, a Program “must address financial, operational, compliance, reputation, and litigation risks” and must be appropriate to the company’s size, complexity, and the nature and scope of its activities.

§ 3:2 Conducting an Initial Risk Assessment

Before a covered entity can identify relevant Red Flags and adopt an Identity Theft Prevention Program, it must first con-
3: Identifying Red Flags

Conduct an initial risk assessment to determine what factors affect the risk of identity theft to customers and the safety and soundness of the financial institution or creditor (financial, operational, compliance, reputation, and litigation risks). Such an assessment will provide a covered entity with a meaningful evaluation of its current identity theft prevention measures; in particular, its shortcomings and risks to its customers.

TIP

Conducting a thorough risk assessment is one of the most important steps to establishing a sound Identity Theft Prevention Program. A deficient risk assessment could well lead to a deficient and ineffective Program.

§ 3:2.1 Practical Considerations

The Rules allow companies the flexibility to adopt policies and procedures that fit their risks. Thus, a risk assessment may not only analyze risk factors, such as the likely circumstances of identity theft, but it also may take into account practical considerations, including the costs and burdens of addressing certain risks. That is not to say that companies may summarily dismiss pertinent Red Flags based on cost. Rather, the Rules provide companies with flexibility to balance costs against risks when determining whether to implement certain Red Flags. Furthermore, as discussed in section 3:4 below, the Rules require that covered entities periodically update their risk assessment to take into account the entity’s own experience with identity theft and to consider changes in the ways accounts are opened and maintained.
§ 3:2.2 Risk Factors to Consider

When conducting a risk assessment to identify relevant Red Flags, financial institutions and creditors must “consider the nature of their business and the type of identity theft to which they may be subject.” The key for any covered entity is to know the facts that apply to them. A covered entity should consider the following risk factors when identifying relevant Red Flags for its covered accounts:

(1) the types of covered accounts it offers or maintains,
(2) the methods it provides to open its covered accounts,
(3) the methods it provides to access its covered accounts, and
(4) its previous experiences with identity theft.6

A risk assessment will reveal those accounts that would be considered “covered accounts” under the Rules, which the Program must address.7 Identifying the types of covered accounts a company offers or maintains allows companies to gauge which of its accounts may be more at risk to identity theft. For example, the threat to deposit accounts likely differs greatly from the threat to credit accounts. Similarly, consumer accounts may be at greater risk than business accounts. Companies also must be aware of whether a business account that it opens or maintains contains any third-party personal information, especially if a business account relates to a sole proprietorship or other small business.

The methods available for customers to open and access accounts also affect the level of risk of identity theft. Accounts that can be opened or accessed remotely will be at greater risk than accounts that must be opened through face-to-face contact with the covered entity’s representatives, and thus require different Red Flags.8
3: Identifying Red Flags

§ 3:2.3 Other Sources to Consider

In addition to the factors mentioned above, the Rules list three other sources of Red Flags that financial institutions and creditors should consider when identifying Red Flags that are relevant to them. The three sources include:

1. incidents of identity theft that the financial institution or creditor has experienced;
2. methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
3. applicable supervisory guidance.

First, a financial institution or creditor should recognize as relevant any Red Flags that directly relate to its prior experiences with identity theft. This requirement applies not only to external threats of identity theft, but also to past experiences of internal problems. For example, past suspicious activities by employees, such as the unauthorized reviewing, exporting, or modifying of customer account information could be identified as possible Red Flags. Red Flags could also be based on any experiences of data breaches, hacking, computer fraud, or any other incidents where lost or stolen data was misappropriated through an external source.

Although it seems obvious that companies should incorporate their own experiences into a Program, this may be a challenge for companies that are not fully aware of their own historical encounters with identity theft. For that reason, instances of data security breaches should be followed by a root cause analysis and review of existing policies. Companies should also have recording systems in place to ensure that their Programs are effective and up-to-date. As we discuss
below in section 3:4, maintaining an updated Program is required under the Rules.

The Rules also refer to applicable supervisory guidance. Applicable supervisory guidance can include alerts or reports distributed by government agencies. The Federal Trade Commission and the Department of Homeland Security provide timely information on their websites regarding identity theft detection and prevention. Government alerts, however, are not the only supervisory guidance available. Trade associations, news reports, and any other public information relating to identity theft trends are a valuable resource, and should be monitored and addressed.

§ 3:3 Categories of Red Flags

Once a company has identified risk factors and possible sources of identity theft, it must identify and list the Red Flags relevant to its size, complexity, and the nature of its activities. Red Flags can vary greatly. After all, a Red Flag is defined broadly as a “pattern, practice, or specific activity that indicates the possible existence of identity theft.”10

The Rules provide twenty-six examples of Red Flags, which fall into five different categories. (See Figure 3A, on pages 28–29.) Incorporation of the Agencies’ examples of Red Flags into the Program is not mandatory. Instead, the Rules
3: Identifying Red Flags

FIGURE 3A:
Examples of Red Flags

<table>
<thead>
<tr>
<th>CATEGORY 1: Warnings from Consumer Reporting Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️ A fraud or active duty alert is included with a consumer report.</td>
</tr>
<tr>
<td>☑️ A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.</td>
</tr>
<tr>
<td>☑️ A consumer reporting agency provides a notice of address discrepancy.</td>
</tr>
<tr>
<td>☑️ A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CATEGORY 2: Suspicious Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️ Documents provided for identification appear to have been altered or forged.</td>
</tr>
<tr>
<td>☑️ The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.</td>
</tr>
<tr>
<td>☑️ Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.</td>
</tr>
<tr>
<td>☑️ 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.</td>
</tr>
<tr>
<td>☑️ An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.</td>
</tr>
</tbody>
</table>
A PRACTICAL GUIDE TO THE RED FLAG RULES

<table>
<thead>
<tr>
<th>CATEGORY 3: Suspicious Personal Identifying Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personal identifying information (“PII”) provided is inconsistent when compared against external information sources used by the financial institution or creditor.</td>
</tr>
<tr>
<td>• PII provided by the customer is not consistent with other PII provided by the customer.</td>
</tr>
<tr>
<td>• PII provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.</td>
</tr>
<tr>
<td>• PII is the same as that submitted by other customers or by an unusually large number of other persons opening an account.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CATEGORY 4: Unusual Use of Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Account used in a manner that is not consistent with historical patterns of activity.</td>
</tr>
<tr>
<td>• Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.</td>
</tr>
<tr>
<td>• A new revolving credit account is used in a manner commonly associated with known patterns of fraud.</td>
</tr>
<tr>
<td>• Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account.</td>
</tr>
<tr>
<td>• A financial institution or creditor is notified that the customer is not receiving paper account statements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CATEGORY 5: Notice from Customers, Law Enforcement or Other Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Customer notifies financial institution or creditor of unauthorized charges.</td>
</tr>
<tr>
<td>• A financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in identity theft.</td>
</tr>
</tbody>
</table>
3: Identifying Red Flags

stick to a “risk-based, non-prescriptive approach regarding the identification of Red Flags . . . , cover a wide variety of financial institutions and creditors that offer and maintain many different products and services, and require flexibility to be able to adapt to rapidly changing risks of identity theft.” Covered entities, therefore, can adopt certain of the example Red Flags as they deem appropriate. Nevertheless, companies should use the categories provided by the Agencies when identifying and listing relevant Red Flags.

The five categories of Red Flags outlined in the Rules are:

(1) alerts, notifications, or warnings received from service providers or consumer reporting agencies,

(2) presentation of suspicious documents,

(3) presentation of suspicious personal identifying information,

(4) unusual use of, or suspicious activity related to, a covered account, and

(5) notifications or reports from consumers, victims of identity theft, law enforcement authorities, or others.

Identifying Red Flags that are not applicable to a particular financial institution or creditor can sometimes be obvious. For instance, if a company does not receive or use consumer reports, then it does not need to list Red Flags for address discrepancy notices received from consumer reporting agencies. If a company does not have face-to-face contact with customers to open or maintain accounts, and does not plan to require face-to-face contact in the future, then the company may not need to incorporate Red Flags related to the presentation of suspicious picture identification documents into its Program.
Nevertheless, if the company does not require face-to-face contact but requires the production of a copy of identification, then the company may need Red Flags to address that situation.

On the other hand, choosing actual relevant Red Flags can be more difficult and requires careful consideration of the information provided through a comprehensive risk assessment. The agencies did not intend for the list of example Red Flags to be an exhaustive list of all the identity theft Red Flags that a financial institution or creditor could experience. Instead, a covered entity is expected to use the risk assessment to develop Red Flags based on the nature, the type, and the complexity of its business.

§ 3:4 Requirement to Update Risks Based on New Threats

Each financial institution and creditor will determine which of its accounts will be covered by its Program by conducting a risk assessment as discussed above. As part of the Program, each financial institution and creditor is required to periodically determine—by conducting additional risk assessments—whether it offers or maintains covered accounts that are subject to the Rules.

Companies must also continuously update their list of Red Flags. With changes in technology, some Red Flags that are relevant to current industry risks may be obsolete in a few years. New types of threats continue to arise as technology changes.
3: Identifying Red Flags

relevant to current industry risks may be obsolete in a few years as new types of threats arise. Although companies are not required to guess what new threats may be looming over the horizon, the Rules clearly intend for covered entities to be mindful of changes in identity theft risks. For example, companies should look to applicable supervisory guidelines to determine what government agencies or industry associations are identifying as new threats. Also, companies should incorporate their own experiences with potential or actual identity theft to ensure that their Program is up-to-date.
Endnotes

1. The Rule is cross-referenced with the FTC’s rule defining identity theft for the purposes of FCRA. See App. A2 infra.
2. § _.90(b)(8); 16 C.F.R. § 603.2(b) (2004).
3. § _.90(b)(9); see App. A2 infra.
4. 72 Fed. Reg. at 63,724 (commentary to § _.90(d)(1)).
6. Appendix J to Part ___; see App. A3 infra.
7. See supra section 2:4 for definition of a “covered account.”
8. 72 Fed. Reg. at 63,727 (commentary to § _.90(d)(2)(i)).
9. Appendix J to Part ___; see App. A3 infra.
10. See section 3:1.2 supra.
11. Supplement A to Appendix J to Part ___; see App. A4 infra.
12. 72 Fed. Reg. at 63,727 (commentary to § _.90(d)(2)(i)).
13. Appendix J to Part ___; see App. A3 infra.