



Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

Tags: [Finance](#) | [Privacy and Security](#) | [Data Security](#) | [Red Flags Rule](#)

An estimated nine million Americans have their identities stolen each year. Identity thieves may drain accounts, damage credit, and even put medical treatment at risk. The cost to business — left with unpaid bills racked up by scam artists — can be staggering, too.

The Red Flags Rule¹ requires many businesses and organizations to implement a written identity theft prevention program designed to detect the “red flags” of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage. The bottom line is that a program can help businesses spot suspicious patterns and prevent the costly consequences of identity theft.

The Federal Trade Commission (FTC) enforces the Red Flags Rule with several other agencies. This article has tips for organizations under FTC jurisdiction to determine whether they need to design an identity theft prevention program.

Table of Contents

- [An Overview](#)
- [Who Must Comply with the Red Flags Rule](#)
- [FAQs](#)
- [How To Comply: A Four-Step Process](#)
- [Endnotes](#)

An Overview

The Red Flags Rule tells you how to develop, implement, and administer an identity theft prevention program. A program must include four basic elements that create a framework to deal with the threat of identity theft.²

1. A program must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft.³ For example, if a customer has to provide some form of identification to open an account with your company, an ID that doesn't look genuine is a “red flag” for your business.
2. A program must be designed to detect the red flags you've identified. If you have identified fake IDs as a red flag, for example, you must have procedures to detect possible fake, forged, or altered identification.
3. A program must spell out appropriate actions you'll take when you detect red flags.
4. A program must detail how you'll keep it current to reflect new threats.

Just getting something down on paper won't reduce the risk of [identity theft](#). That's why the Red Flags Rule has requirements on how to incorporate your program into the daily operations of your business. Fortunately, the Rule also gives you the flexibility to design a program appropriate for your company — its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive program to address a high risk of identity theft, a streamlined program may be appropriate for businesses facing a low risk.

Securing the data you collect and maintain about customers is important in reducing identity theft. The Red Flags Rule seeks to prevent identity theft, too, by ensuring that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get products or services from you without paying for them. That's why it's important to use a one-two punch in the battle against identity theft: implement data security practices that make it harder for crooks to get access to the personal information they use to open or access accounts, and pay attention to the red flags that suggest that fraud may be afoot.

Who Must Comply with the Red Flags Rule: A Two-Part Analysis

The Red Flags Rule requires “financial institutions” and some “creditors” to conduct a periodic risk assessment to determine if they have “covered accounts.” The determination isn't based on the industry or sector, but rather on whether a business' activities fall within the relevant definitions. A business must implement a written program **only** if it has covered accounts.

Financial Institution

The Red Flags Rule defines a “financial institution” as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or a person that, directly or indirectly, holds a transaction account belonging to a consumer.⁴ While many financial institutions are under the jurisdiction of the federal bank regulatory agencies or other federal agencies, state-chartered credit unions are one category of financial institution under the FTC's jurisdiction.

Creditor

The Red Flags Rule defines “creditor” based on conduct.⁵

To determine if your business is a creditor under the Red Flags Rule, ask these questions:

Does my business or organization regularly:

- defer payment for goods and services or bill customers?
- grant or arrange credit?
- participate in the decision to extend, renew, or set the terms of credit?

If you answer:

- No to all, the Rule does not apply.
- Yes to one or more, ask:

Does my business or organization regularly and in the ordinary course of business:

- get or use consumer reports in connection with a credit transaction?
- give information to credit reporting companies in connection with a credit transaction?
- advance funds to — or for — someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)?

If you answer:

- No to all, the Rule does not apply.
- Yes to one or more, you are a creditor covered by the Rule.

Covered Accounts

If you conclude that your business or organization is a financial institution or a creditor covered by the Rule, you must determine if you have any “covered accounts,” as the Red Flags Rule defines that term. You’ll need to look at existing accounts **and** new ones⁶. Two categories of accounts are covered:

1. A consumer account for your customers for personal, family, or household purposes that involves or allows multiple payments or transactions.⁷ Examples are credit card accounts, mortgage loans, automobile loans, checking accounts, and savings accounts.
2. “Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.”⁸ Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to allow multiple payments or transactions — always considered “covered accounts” under the Rule — other types of accounts are “covered” only if the risk of identity theft is reasonably foreseeable.

In determining if accounts are covered under the second category, consider how they’re opened and accessed. For example, there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely — say, through the Internet or the telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these.

If you don’t have any covered accounts, you don’t need a written program. But business models and services change. You may acquire covered accounts through changes to your business structure, process, or organization. That’s why it’s good policy and practice to conduct a periodic risk assessment.

FAQs

1. **I review credit reports to screen job applicants. Does the Rule apply to my business on this basis alone?**

No, the Rule does not apply because the use is not “in connection with a credit transaction.”

2. **What if I *occasionally* get credit reports in connection with credit transactions?**

According to the Rule, these activities must be done “regularly and in the ordinary course of business.” Isolated conduct does not trigger application of the Rule, but if your business regularly furnishes delinquent account information to a consumer reporting company but no other credit information, that satisfies the “regularly and in the ordinary course of business” prerequisite.

What is deemed “regularly and in the ordinary course of business” is specific to individual companies. If you get consumer reports or furnish information to a consumer reporting company regularly and in the ordinary course of your particular business, the Rule applies, even if for others in your industry it isn’t a regular practice or part of the ordinary course of business.

3. I am a professional who bills my clients for services at the end of the month. Am I a creditor just because I allow clients to pay later?

No. Deferring payment for goods or services, payment of debt, or the purchase of property or services alone doesn’t constitute “advancing funds” under the Rule.

4. In my business, I lend money to customers for their purchases. The loans are backed by title to their car. Is this considered “advancing funds”?

Yes. Anyone who lends money — like a payday lender or automobile title lender — is covered by the Rule. Their lending activities may make their business attractive targets for identity theft. But deferring the payment of debt or the purchase of property or services alone doesn’t constitute “advancing funds.”

5. I offer instant credit to my customers and contract with another company to pull credit reports to determine their creditworthiness. No one in our organization ever sees the credit reports. Is my business covered by the Rule?

Yes. Your business is — regularly and in the ordinary course of business — using credit reports in connection with a credit transaction. The Rule applies whether your business uses the reports directly or whether a third-party evaluates them for you.

6. I operate a finance company that helps people buy furniture. Does the Rule apply to my business?

Yes. Your company’s financing agreements are considered to be “advancing funds on behalf of a person.”

7. In my legal practice, I often make copies and pay filing, court, or expert fees for my clients. Am I “advancing funds”?

No. This is not the same as a commercial lender making a loan; “advancing funds” does not include paying in advance for fees, materials, or services that are incidental to providing another service that someone requested.

8. Our company is a “creditor” under the Rule and we have credit and non-credit accounts. Do we have to determine if both types of accounts are “covered accounts”?

Yes. You must examine all your accounts to determine which are “covered accounts” that must be included in your written identity theft prevention program.

9. My business accepts credit cards for payments. Are we covered by the Red Flags Rule on this basis alone?

No. Just accepting credit cards as a form of payment does not make you a “creditor” under the Red Flags Rule.

10. My business isn’t subject to much of a risk that a crook is going to misuse someone’s identity to steal from me, but it does have covered accounts. How should I structure my program?

If identity theft isn’t a big risk in your business, complying with the Rule is simple and straightforward. For example, if the risk of identity theft is low, your program might focus on how to respond if you are notified — say, by a customer or a law enforcement officer — that someone’s identity was misused at your business. The Guidelines to the Rule have examples of

possible responses. But even a business at low risk needs a written program that is approved either by its board of directors or an appropriate senior employee.

How To Comply: A Four-Step Process

Many companies already have plans and policies to combat identity theft and related fraud. If that's the case for your business, you're already on your way to full compliance.

1. Identify Relevant Red Flags

What are "red flags"? They're the potential patterns, practices, or specific activities indicating the possibility of identity theft.² Consider:

Risk Factors. Different types of accounts pose different kinds of risk. For example, red flags for deposit accounts may differ from red flags for credit accounts, and those for consumer accounts may differ from those for business accounts. When you are identifying key red flags, think about the types of accounts you offer or maintain; the ways you open covered accounts; how you provide access to those accounts; and what you know about identity theft in your business.

Sources of Red Flags. Consider other sources of information, including the experience of other members of your industry. Technology and criminal techniques change constantly, so it's important to keep up-to-date on new threats.

Categories of Common Red Flags. Supplement A to the Red Flags Rule lists specific categories of warning signs to consider including in your program. The examples here are one way to think about relevant red flags in the context of your own business.

- **Alerts, Notifications, and Warnings from a Credit Reporting Company.** Changes in a credit report or a consumer's credit activity might signal identity theft:
 - a fraud or active duty alert on a credit report
 - a notice of credit freeze in response to a request for a credit report
 - a notice of address discrepancy provided by a credit reporting company
 - a credit report indicating a pattern inconsistent with the person's history B for example, an increase in the volume of inquiries or the use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account that was closed because of an abuse of account privileges
- **Suspicious Documents.** Documents can offer hints of identity theft:
 - identification looks altered or forged
 - the person presenting the identification doesn't look like the photo or match the physical description
 - information on the identification differs from what the person with identification is telling you or doesn't match a signature card or recent check
 - an application looks like it's been altered, forged, or torn up and reassembled
- **Personal Identifying Information.** Personal identifying information can indicate identity theft:
 - inconsistencies with what you know — for example, an address that doesn't match the credit report or the use of a Social Security number that's listed on the Social Security

Administration Death Master File

- inconsistencies in the information a customer has submitted to you
- an address, phone number, or other personal information already used on an account you know to be fraudulent
- a bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service
- a Social Security number used by someone else opening an account
- an address or telephone number used by several people opening accounts
- a person who omits required information on an application and doesn't respond to notices that the application is incomplete
- a person who can't provide authenticating information beyond what's generally available from a wallet or credit report — for example, someone who can't answer a challenge question
- **Account Activity.** How the account is being used can be a tip-off to identity theft:
 - shortly after you're notified of a change of address, you're asked for new or additional credit cards, or to add users to the account
 - a new account used in ways associated with fraud — for example, the customer doesn't make the first payment, or makes only an initial payment; or most of the available credit is used for cash advances or for jewelry, electronics, or other merchandise easily convertible to cash
 - an account used outside of established patterns — for example, nonpayment when there's no history of missed payments, a big increase in the use of available credit, or a major change in buying or spending patterns or electronic fund transfers
 - an account that is inactive is used again
 - mail sent to the customer that is returned repeatedly as undeliverable although transactions continue to be conducted on the account
 - information that the customer isn't receiving an account statement by mail or email
 - information about unauthorized charges on the account
- **Notice from Other Sources.** A customer, a victim of identity theft, a law enforcement authority, or someone else may be trying to tell you that an account has been opened or used fraudulently.

2. Detect Red Flags

Sometimes, using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online.

- **New accounts.** When verifying the identity of the person who is opening a new account, reasonable procedures may include getting a name, address, and identification number and, for in-person verification, checking a current government-issued identification card, like a driver's license or passport. Depending on the circumstances, you may want to compare that to information you can find out from other sources, like a credit reporting company or data broker, or the Social Security Number Death Master File.¹⁰ Asking questions based on information from other sources can be a helpful way to verify someone's identity.

- **Existing accounts.** To detect red flags for existing accounts, your program may include reasonable procedures to confirm the identity of the person you're dealing with, to monitor transactions, and to verify the validity of change-of-address requests. For online authentication, consider the Federal Financial Institutions Examination Council's guidance on authentication as a starting point.¹¹ It explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PINs, smart cards, tokens, and biometric identification. Certain types of personal information — like a Social Security number, date of birth, mother's maiden name, or mailing address — are not reliable authenticators because they're so easily accessible.

You may be using programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. If so, incorporate these tools into your program.

3. Prevent And Mitigate Identity Theft

When you spot a red flag, be prepared to respond appropriately. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service.

The Guidelines in the Red Flags Rule offer examples of some appropriate responses, including:

- monitoring a covered account for evidence of identity theft
- contacting the customer
- changing passwords, security codes, or other ways to access a covered account
- closing an existing account
- reopening an account with a new account number
- not opening a new account
- not trying to collect on an account or not selling an account to a debt collector
- notifying law enforcement
- determining that no response is warranted under the particular circumstances

The facts of a particular case may warrant using one of these options, several of them, or another response altogether. Consider whether any aggravating factors raise the risk of identity theft. For example, a recent breach that resulted in unauthorized access to a customer's account records would call for a stepped-up response because the risk of identity theft rises, too.

4. Update The Program

The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics, and requires periodic updates to your program. Factor in your own experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

Administering Your Program

Your Board of Directors — or an appropriate committee of the Board — must approve your initial plan. If you don't have a board, someone in senior management must approve it. The Board may oversee, develop, implement, and administer the program — or it may designate a senior employee to do the job. Responsibilities include assigning specific responsibility for the program's implementation, reviewing staff reports about compliance with the Rule, and approving important changes to your program.

The Rule requires that you train relevant staff only as “necessary.” Staff who have taken fraud prevention training may not need to be re-trained. Remember that employees at many levels of your organization can play a key role in identity theft deterrence and detection.

In administering your program, monitor the activities of your service providers. If they're conducting activities covered by the Rule — for example, opening or managing accounts, billing customers, providing customer service, or collecting debts — they must apply the same standards you would if you were performing the tasks yourself. One way to make sure your service providers are taking reasonable steps is to add a provision to your contracts that they have procedures in place to detect red flags and either report them to you or respond appropriately to prevent or mitigate the crime. Other ways to monitor your service providers include giving them a copy of your program, reviewing the red flag policies, or requiring periodic reports about red flags they have detected and their response.

It's likely that service providers offer the same services to a number of client companies. As a result, the Guidelines are flexible about service providers using their own programs as long as they meet the requirements of the Rule.

The person responsible for your program should report at least annually to your Board of Directors or a designated senior manager. The report should evaluate how effective your program has been in addressing the risk of identity theft; how you're monitoring the practices of your service providers; significant incidents of identity theft and your response; and recommendations for major changes to the program.¹²

FTC Resources

Identity Theft

ftc.gov/idtheft

Endnotes

¹ The Red Flags Rule was issued in 2007 under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Pub. L. 108-159, amending the Fair Credit Reporting Act (FCRA), 15 U.S.C. ' 1681m(e). The Red Flags Rule is published at 16 C.F.R. ' 681.1. See also 72 Fed. Reg. at 63,771 (Nov. 9, 2007). You can find the full text at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf> . The preamble B pages 63,718-63,733 — discusses the purpose, intent, and scope of coverage of the Rule. The text of the FTC rule is at pages 63,771-63,774. The Rule includes Guidelines B Appendix A, pages 63,773-63,774 — intended to help businesses develop and maintain a compliance program. The Supplement to the Guidelines — page 63,774 — provides a list of examples of red flags for businesses and organizations to consider incorporating into their program. This guide does not address companies' obligations under the Address Discrepancy or the Card Issuer Rule, also contained in the Federal Register with the Red Flags Rule.

The Rule was amended in 2010 by the Red Flag Program Clarification Act of 2010, 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457 (Dec. 18, 2010).

2 "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. See 16 C.F.R. ' 603.2(a). "Identifying information" means "any 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))."

See 16 C.F.R. ' 603.2(b).

3 See 16 C.F.R. ' 681.1(b)(9).

4 The Rule definition of "financial institution" is found in the FCRA. See 15 U.S.C. ' 1681a(t). The term "transaction" is defined in section 19(b) of the Federal Reserve Act. See 12 U.S.C. ' 461(b)(1)(C). A "transaction account" is a deposit or account from which owners may make payments or transfers to third parties or others. Transaction accounts include checking accounts, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

5 "Creditor" and "credit" are defined in the FCRA, see 15 U.S.C. 1681a(r)(5), by reference to section 702 of the Equal Credit Opportunity Act (ECOA), 15 U.S.C. ' 1691a. The ECOA defines "credit" as "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor." 15 U.S.C. ' 1691a(d). The ECOA defines "creditor" as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of any original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C. ' 1691a(e). The term "person" means "a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association." 15 U.S.C. ' 1691a(f). See also Regulation B. 68 Fed. Reg. 13,161 (Mar. 18, 2003).

The Clarification Act has modified the definition of "creditor" however. For purposes of the Red Flags Rule, a creditor —

"A. means a creditor, as defined in section 702 of the [ECOA], that regularly and in the ordinary course of business—

(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

(ii) furnishes information to consumer reporting agencies, as described in section 623 [of the FCRA], in connection with a credit transaction; or

(iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;

B. does not include a creditor ... that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person."

6 An “account” is 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. 16 C.F.R. ' 681.1(b)(1). An account does not include a one-time transaction involving someone who isn't your customer, such as a withdrawal from an ATM machine.

7 See 16 C.F.R. ' 681.1(b)(3)(i).

8 16 C.F.R. ' 681.1(b)(3)(ii).

9 See 16 C.F.R. ' 681.12(b)(9).

10 The verification procedures are set forth in the Customer Identification Programs Rule applicable to banking institutions, 31 C.F.R. ' 103.121. This Rule may be a helpful starting point in developing your program.

11 “Authentication in an Internet Banking Environment” (Oct. 2, 2005) available at http://www.ffiec.gov/pdf/authentication_guidance.pdf .

12 See 72 Fed. Reg. at 63,773.

May 2013