FIGHTING FRAUD
WITH THE RED FLAGS RULE
A How-To Guide for Business
FIGHTING THE RED FLAGS
A How-To Guide

As many as nine million identities are stolen each year. Identity thieves can damage their credit, costing their victims treatment. The cost of cleaning up the mess can be staggering.

The “Red Flags” Rule of the Federal Trade Commission (FTC) and the National Credit Reporting agencies requires many businesses to detect the warning signs of identity theft in their day-to-day transactions and prevent the crime, as well as to take steps to prevent a costly episode of identity theft.

The Red Flags Rule, issued by the FTC, provides guidance to organizations that work for a bank, federal savings and loan, credit agency or any other company for designing your Identity Theft Prevention Plan.

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW, Washington, DC 20580
ftc.gov/redflagsrule
THE RED FLAGS RULE
An Overview

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs. Your Program must include four basic elements, which together create a framework to address the threat of identity theft.2

First, your Program must include reasonable policies and procedures to identify the “red flags” of identity theft you may run across in the day-to-day operation of your business. 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 looks like it might be fake would be a “red flag” for your business.

Second, your Program must be designed to detect the red flags you’ve identified. For example, if you’ve identified fake IDs as a red flag, you must have procedures in place to detect possible fake, forged, or altered identification.

Third, your Program must spell out appropriate actions you’ll take when you detect red flags.

Fourth, because identity theft is an ever-changing threat, you must address how you will re-evaluate your Program periodically to reflect new risks from this crime.

Just getting something down on paper won’t reduce the risk of identity theft. That’s why the Red Flags Rule sets out requirements on how to incorporate your Program into the daily operations of your business. Your board of directors (or a committee of the board) has to approve your first written Program. If you don’t have a board, approval is up to an appropriate senior-level employee. Your Program must state who’s responsible for implementing and administering it effectively. Because your employees have a role to play in preventing and detecting identity theft, your Program must include appropriate staff training. You may also subcontract parts of your operation. The Red Flags Rule, your Program also must address contractors’ compliance.

The Red Flags Rule gives you the flexibility to develop an appropriate Program for your company — one that addresses the specific risks faced by your business. While some businesses may need a comprehensive Program that addresses a complex organization, others may have a more streamlined Program that meets their needs.
QUESTION: How does the Red Flags Rule fit in with the data security measures we’re already taking?

ANSWER:
Preventing identity theft requires a 360° approach. Data security plays an essential role in keeping people’s sensitive information from falling into the wrong hands. Protect what you have a legitimate business reason to keep and securely dispose of what you no longer need. But even with appropriate data security measures in place, thieves are resourceful and still may find ways to steal information and use it to open or access accounts. That hurts individual identity theft victims, who may have to spend hundreds of dollars and many days repairing damage to their good name and credit record. But it also hurts your bottom line. Identity thieves run up huge bills with no intention of paying – leaving you with accounts receivable you’ll never be able to collect.

The Red Flag Rule picks up where data security leaves off. It seeks to prevent identity theft 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 with no intention of paying. That’s why it’s important to fight the battle against identity theft on two fronts: First, by implementing data security practices that make it harder for crooks to get access to the personal information they use to open or access accounts, and second, by paying attention to the red flags that suggest that fraud may be afoot. For more on how to implement data security protections in your business, visit ftc.gov/infosecurity.
WHO MUST COMPLY WITH THE RED FLAGS RULE

The Red Flags Rule applies to “creditors.” The Rule requires you to assess whether your business or organization is covered by the Rule by conducting an assessment to determine if you need to implement a written program to comply with its requirements.

It’s important to look closely at what constitutes an “institution” and “creditor” because it might not typically use those words. For example, many non-profit groups might not consider themselves “creditors” under the Rule. The determination of whether your business or organization is covered by the Red Flags Rule isn’t based on your industry or sector, but rather on whether your activities fall within the relevant definitions.

Financial Institution The definition of “financial institution” as a state or national bank, savings and loan association, a mutual savings bank, credit union, or any other person that issues a transaction account belonging to a state-chartered credit unions, and savings associations, and under the jurisdiction of the federal government and/or the National Credit Union Administration. Financial institutions come under the purview of the Federal Trade Commission and federal agencies for guidance tailored to their activities. Examples of financial institutions include state-chartered credit unions, mutual savings banks, check-writing privileges, or other accounts where the consumer can make payments.

Creditor The definition of “creditor” includes businesses or organizations that offer products or services or provide goods or services or provide goods or services or provide goods or services. Utility companies, health care providers, and companies are among the entities.
The second kind of “covered account” for a financial institution or creditor is a reasonably foreseeable risk to the financial institution’s soundness, including financial, operational, or reputational risks.9 Examples include small accounts, or single transaction accounts vulnerable to identity theft. Under the Rule, “covered accounts” only if the risk of identity theft is a reasonably foreseeable risk.

In determining if accounts are “covered,” you must consider how they’re opened and operated. If accounts can be opened remotely, such as over the Internet or by telephone. Your business must evaluate both types of accounts to determine if they are covered.

Covered Accounts Once you’ve concluded that your business or organization is a financial institution or creditor, you must determine if you have any “covered accounts” as the Red Flags Rule defines that term. To make that determination, you’ll need to look at both existing accounts and new ones. Two categories of accounts are covered.7

The first kind is a consumer account you offer your customers that’s primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.8 Examples are credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

QUESTION: I know our company that has account rendered (credit accounts) when service is rendered (non-transaction accounts) is a financial institution or creditor under the Red Flags Rule because we regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions. Examples include finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers get financing from others, say, by processing credit applications. In addition, the definition includes anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit – for example, a third-party debt collector who regularly renegotiates the terms of a debt. If you regularly extend credit to other businesses, you also are covered under this definition.

The Rule also defines a “creditor” as one who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions. Examples include finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers get financing from others, say, by processing credit applications. In addition, the definition includes anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit – for example, a third-party debt collector who regularly renegotiates the terms of a debt. If you regularly extend credit to other businesses, you also are covered under this definition.

Covered Accounts Once you’ve concluded that your business or organization is a financial institution or creditor, you must determine if you have any “covered accounts,” as the Red Flags Rule defines that term. To make that determination, you’ll need to look at both existing accounts and new ones. Two categories of accounts are covered.

The first kind is a consumer account you offer your customers that’s primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

QUESTION: I manage a restaurant that accepts credit cards. Are we covered by the Red Flags Rule?

ANSWER: Probably not. Simply accepting credit cards as a form of payment does not make you a “creditor” under the Red Flags Rule. But if a company offers its own credit card, arranges credit for its customers, or extends credit by selling customers goods or services now and billing them later, it is a “creditor” under the law.
QUESTION:
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 I do have covered accounts. How should I structure my Program?

ANSWER:
If identity theft isn’t a big risk in your business, complying with the Rule should be simple and straightforward, with only a few red flags. For example, where the risk of identity theft is low, your Program might focus on how to respond if you are notified – say, by a consumer or a law enforcement officer – that the person’s identity was misused at your business. The Guidelines to the Rule have examples of possible responses. But even a low-risk business needs to have a written Program that is approved either by its board of directors or an appropriate senior employee. And because risks change, you must assess your Program periodically to keep it current.

Don’t have any covered accounts? You don’t need to have a written Program. But business models and services change. That’s why you must conduct a periodic risk assessment to help you determine if you’ve acquired any covered accounts through changes to your business structure, processes, or organization.
HOW TO COMPLY: A FOUR STEP PROCESS

step 1
Identify relevant red flags.
Identify the red flags of identity theft you’re likely to come across in your business.

step 2
Detect red flags.
Set up procedures to detect those red flags in your day-to-day operations.

step 3
Prevent and mitigate identity theft.
If you spot the red flags you’ve identified, respond appropriately to prevent and mitigate the harm done.

If you’re a creditor or financial institution with covered accounts, you must develop and implement a written Identity Theft Prevention Program. The Program must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones. Your Program must be appropriate to the size and complexity of your business or organization and the nature and scope of its activities. A company with a higher risk of identity theft or a variety of covered accounts may need a more comprehensive Program.

Many companies already have plans in place to combat identity theft and related fraud. If that’s the case for your business, you may be able to incorporate procedures that already have proven effective.
Although there's no one-size-fits-all approach, consider:

- **Risk Factors**
- **Sources of Red Flags**
- **Categories of Common Red Flags**

**What are “red flags”?** They’re the or specific activities indicating the Although there’s no one-size-fits-

**Risk Factors** Different types of risk. For example, red flags from red flags for credit account consumer accounts may not be accounts. And red flags for ac or by phone may differ from th. Therefore, in identifying the rel of accounts you offer or maint covered accounts; how you provide what you have learned about id.

**Sources of Red Flags** Cons information, including how id business and the experience of o. Because technology and crime keep up-to-date on new threats.

**Categories of Common Red** Red Flags Rule lists five specific consider including in your Pro relevant to your business or on only when combined or cons identity theft. The examples, li an exhaustive compilation or a way to help think about rele your business.
1. Alerts, Notifications, and Credit Reporting

Here are some examples of consumer’s credit activity that may indicate fraud or active duty alert:

- a fraud or active duty alert
- a notice of credit freeze in a credit report
- a notice of address discrepancy with the reporting agency
- a credit report indicating volume of inquiries or the accounts; an unusual number of relationships; or an account abuse of account privilege

2. Suspicious Documents

Sometimes paperwork has to be looked at more closely. Here are examples of red flags:

- identification that looks as if it has been cut or torn up and reassembled
- the person presenting the photo or match the photo
- information on the identification that doesn’t match with other personal or recent check
- an application that looks as if it has been cut or torn up and reassembled
3. Suspicious Personal Identifying Information.

Identity thieves may use personally identifying information that doesn’t ring true. Here are some red flags involving identifying information:

- inconsistencies with what else you know – for example, an address that doesn’t match the credit report, the use of a Social Security number that’s listed on the Social Security Administration Death Master File, or a number that hasn’t been issued, according to the monthly issuance tables available from the Social Security Administration

- inconsistencies in the information the customer has given you – say, a date of birth that doesn’t correlate to the number range on the Social Security Administration’s issuance tables

- an address, phone number, or other personal information that’s been 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 that’s been used by someone else opening an account

- an address or telephone number that’s been used by many other 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, a person who can’t answer a challenge question

4. Suspicious Account Activity

Sometimes the tip-off is how some red flags related to account activity:

- soon after you’re notified for new or additional users to the account

- a new account that’s used for cash advances, merchandise easily converted

- a person who makes only an initial purchase

- electronic fund transfers

- a Social Security number that’s been used by someone else opening an account

- an account that’s been used again

- mail sent to the customer undeliverable although statements in the mail

- a person who can’t provide authenticating information beyond what’s generally available from a wallet or credit report

5. Notice from Other Sources

Sometimes a red flag that a fraudulently can come from a law enforcement authority...
Detect Red Flags

Once you’ve identified the red flags of identity theft for your business, it’s time to lay out procedures for detecting them in your day-to-day operations. Sometimes using identity verification and authentication methods can help you turn up red flags. Consider how your procedures may differ depending on whether an identity verification or authentication is taking place in person or at a distance – say, by telephone, mail, Internet, or wireless system.

New accounts When verifying opening a new account, reason a name, address, and identification verification, checking a current like a driver’s license or passport you may want to compare that you can find out from other source or data broker, the Social Security publicly available information. You on information from other source someone’s identity.

Existing accounts To detect your Program may include reason customers (confirming that the is your customer), monitor transaction change-of-address requests. For Federal Financial Institutions Federal authentication as a starting point, multi-factor authentication techniques including using passwords, PIN biometric identification. Certain like a Social Security number, or mailing address – are not go easily accessible.

You may already be using program behavior that indicates the possible validate changes of address. If the into your Program.
PREVENT AND MITIGATE
IDENTITY THEFT

When you spot a red flag, be prepared to respond appropriately. Your response will depend upon the degree of risk posed. It may need to accommodate other legal obligations – for example, laws for medical providers or utility companies regarding the provision and termination of 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 or several of these options, or another response altogether. In determining your response, consider whether any aggravating factors heighten the risk of identity theft. For example, a recent breach that resulted in unauthorized access to a customer’s account records or a customer who gave personal information to an imposter would certainly call for a stepped-up response because the risk of identity theft would go up.

UPDATE THE PROGRAM

The Rule recognizes that new red flags or identity thieves change their methods, so updates to your Program to ensure that you can prevent and mitigate identity theft; changes in your business, such as mergers, ventures, and arrangements with others.
ADMINISTERING YOUR PROGRAM

Your initial written Program must get the approval of your board of directors or an appropriate committee of the board; if you don’t have a board, someone in senior management must approve it.

Your 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 the organization is complying with changes to your Program.

The Rule requires that you train, for example, staff that has received may not need to be re-trained. many levels of your organization deterrence and detection.

In administering your Program providers. If they’re conducting for example, opening or managing customer service, or collecting or standards you would if you were way to make sure your service provider is to add a provision to your company place to detect red flags and either appropriately to prevent or mitigate ways to monitor them include reviewing their red flags policy; red flags they have detected and

It’s likely that service providers client companies. As a result, the service providers that have their the requirements of the Rule.

The person responsible for your to the board of directors or a des should evaluate how effective you the risk of identity theft; how your service providers; significant inc response; and recommendations
RESOURCES

For more information on developing your Identity Theft Prevention Program:

New “Red Flag” Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft
ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

The “Red Flags” Rule: Are You Complying with New Requirements for Fighting Identity Theft?
ftc.gov/bcp/edu/pubs/articles/art10.shtm

The Red Flags Rule

Find out about identity theft and data security:

The FTC’s Identity Theft Site
ftc.gov/idtheft

OnGuard Online Identity Theft Site
onguardonline.gov/topics/identity-theft.aspx

The FTC’s Information Security Site
ftc.gov/infosecurity

Protecting Personal Information:
A Guide for Business
ftc.gov/bcp/edu/pubs/business/IDTHFT/bus69.pdf

Information Security Interactive Video Tutorial
ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html
ENDNOTES


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).


5. The Rule’s definition of “financial institution” is found in the FCRA. See 15 U.S.C. § 1681a(f). The term “transaction account” 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 the owner may make payments or transfers to third parties or other accounts, negotiable orders of withdrawal, automatic transfers, and share drafts.

6. “Creditor” and “credit” are defined by reference to section 702 of the U.S.C. § 1691a. The ECOA defines a creditor to a debtor to defer payment of debt, or to purchase property or services for a debtor, or to renew or continue credit; any purchase, renewal, or continuation of credit who participates in the decision to extend beyond a one-time transaction.

7. An “account” is a continuing relationship between a financial institution or creditor to a family, household, or business purpose that does not include a one-time transaction customer, such as a withdrawal from a checking account.


10. See 16 C.F.R. § 681.2(b)(9).

11. The Social Security Administration can buy that contains records of the Social Security Administration. See www.ssa.gov/employer/ssnv

12. See www.ssa.gov/employer/ssnv

13. These verification procedures are available at www.ffiec.gov/press/

14. “Authentication in an Internet Protocol Rule may be a helpful starting point”
