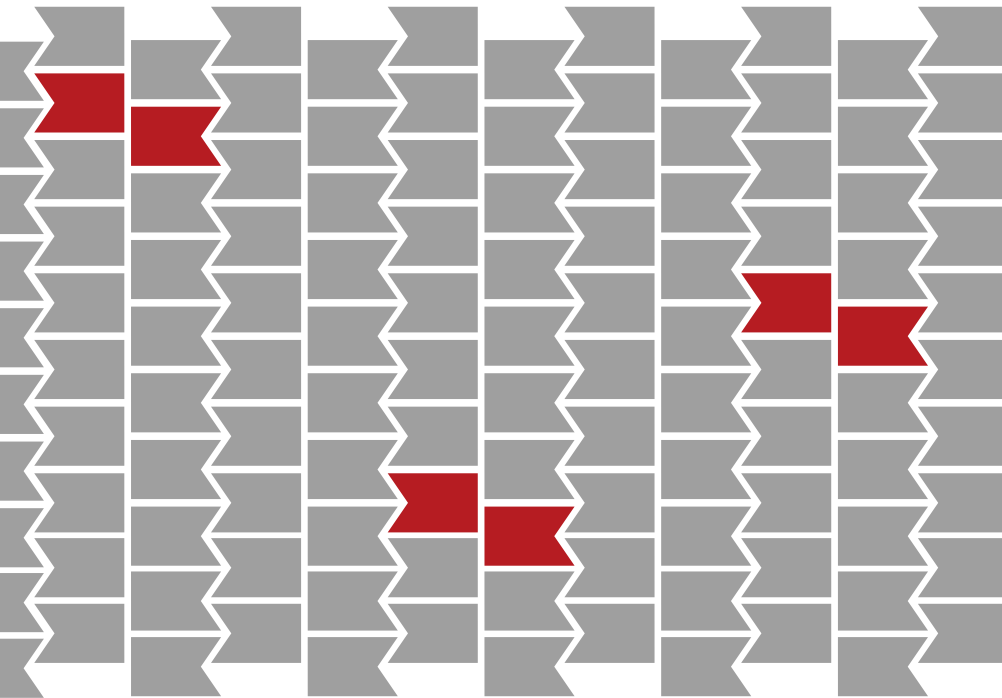


Federal Trade Commission
Protecting America's Consumers



FIGHTING FRAUD WITH THE RED FLAGS RULE

A How-To Guide for Business





FIGHTING THE RED A How-To Guide

As many as nine million mobile phones are stolen each year. Identity thieves can use stolen phones to damage their credit, access bank accounts, and receive medical treatment. The cost of a stolen phone is racked up by scam artists.

The “Red Flags” Rule requires many businesses to provide consumers with a written Identity Theft Notice. This notice helps to detect the warning signs of identity theft in their day-to-day lives and helps to prevent the crime, and reduce the damage. By identifying red flags, consumers are better equipped to spot suspicious activity and can take steps to prevent a costly episode of identity theft.

The Red Flags Rule is enforced by the Federal Trade Commission (FTC) and the National Consumer Financial Protection Agency. If you work for a bank, federal credit union, or savings and loan, check with your agency for guidance on how to comply with the rule. Determining if you are a covered entity is the first step for designing your Red Flags Rule.

FEDERAL TRADE COMMISSION

600 Pennsylvania Avenue, NW, Washington, DC 20580

1-877-FTC-HELP (1-877-382-4357)

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 to monitor and respond to red flags. If you subcontract parts of your operations, the Red Flags Rule, your Program also must address the identity theft risk of your contractors’ compliance.

The Red Flags Rule gives you the flexibility to design a Program appropriate for your company - from a small business to a comprehensive Program that addresses a complex organization, others may have a more streamlined Program.





The Red Flags where data sec



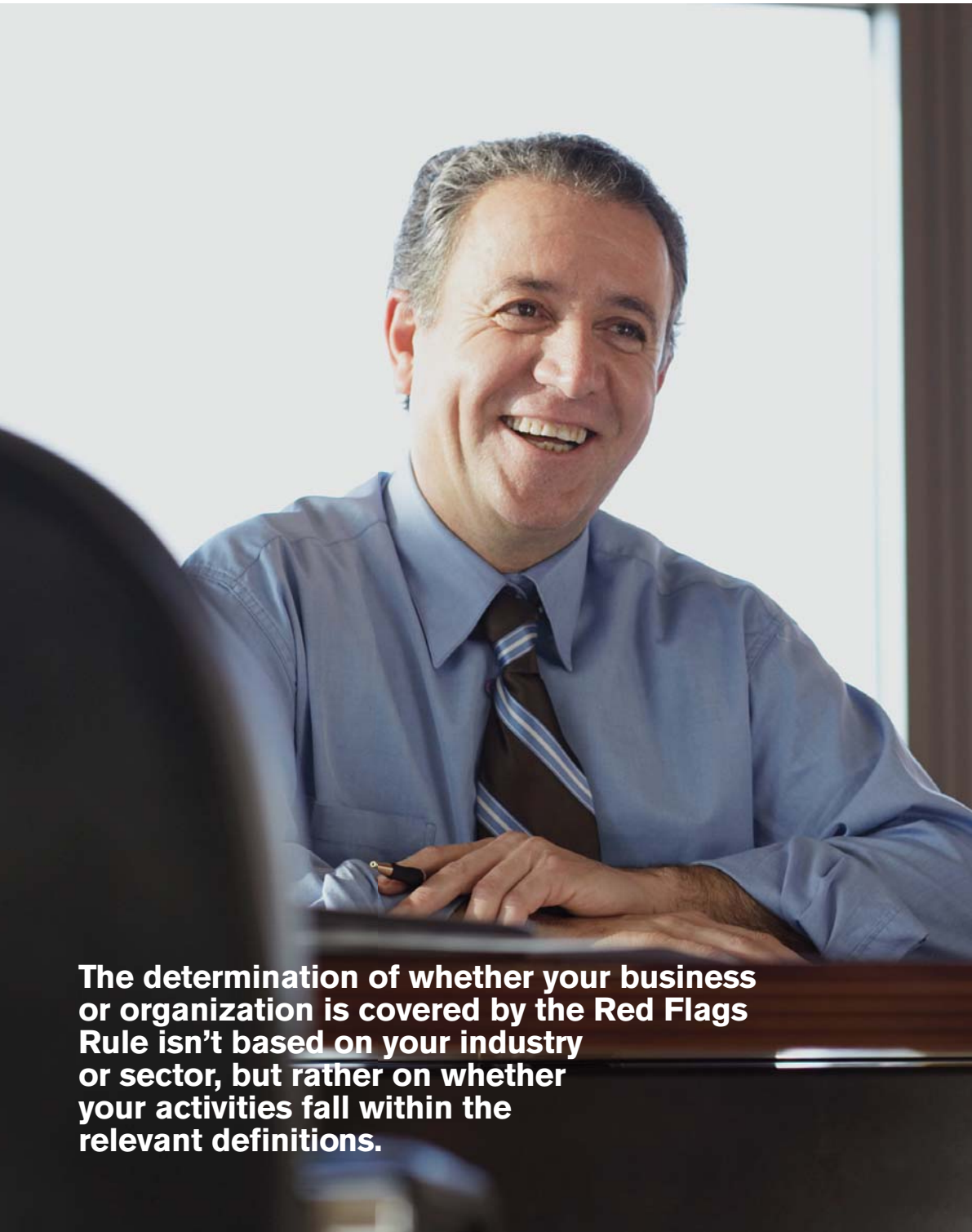
QUESTION:

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.



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.

WHO MUST COMPLY WITH THE RED FLAGS RULE

The Red Flags Rule applies to “creditors.” The Rule requires your assessment to determine if you need to implement a written program.

It's important to look closely at the definition of “financial institution” and “creditor” because you might not typically use those words. For example, many non-profit groups are “creditors” under the Rule.⁴ The Rule applies to your business or organization if you are covered by the Rule on your industry or sector, but only if your activities fall within the relevant definitions.

Financial Institution The Red Flags Rule defines “financial institution” as a state or national bank, a credit union, and loan association, a mutual savings bank, a credit union, or any other person or organization that maintains a transaction account belonging to a consumer. This includes chartered credit unions, and savings and loan associations under the jurisdiction of the federal Reserve and/or the National Credit Union Administration. Agencies for guidance tailored to financial institutions come under the supervision of the FDIC. Examples of financial institutions include state-chartered credit unions, mutual savings banks, check-writing privileges, or other financial services where the consumer can make payments.

Creditor The definition of “creditor” includes businesses or organizations that sell goods or services or provide goods or services. Utility companies, health care providers, and other companies are among the entities that are considered creditors.

definition, depending on how and when they collect payment for their services. 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.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 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.

The second kind of “covered accounts” is a financial institution or creditor account that is a reasonably foreseeable risk to the soundness of the financial institution, including financial, operational, or reputational risks.”⁹ Examples include small business accounts, or single transaction accounts that are vulnerable to identity theft. Under the Rule, you may permit multiple payments or transactions on “covered accounts” under the Rule – other than “single transaction accounts” only if the risk of identity theft is a reasonably foreseeable risk to the soundness of the business accounts that can be accessed by the Internet or by telephone. Your business should evaluate incidents of identity theft involving

QUESTION:
I know our company is covered by the Red Flags Rule because we have credit accounts. But we also have non-transaction accounts. Do we have to determine if those accounts are “covered”?

ANSWER:
Yes, and the same goes for non-transaction accounts and non-transaction accounts. If you are a company that has accounts that are rendered (credit accounts) when service is rendered (non-transaction accounts), you should evaluate both types of accounts. Likewise, a broker-dealer that has accounts that are rendered (transaction accounts) when service is rendered (non-transaction accounts) should evaluate both types of accounts to determine if they are covered.

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.



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.



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.

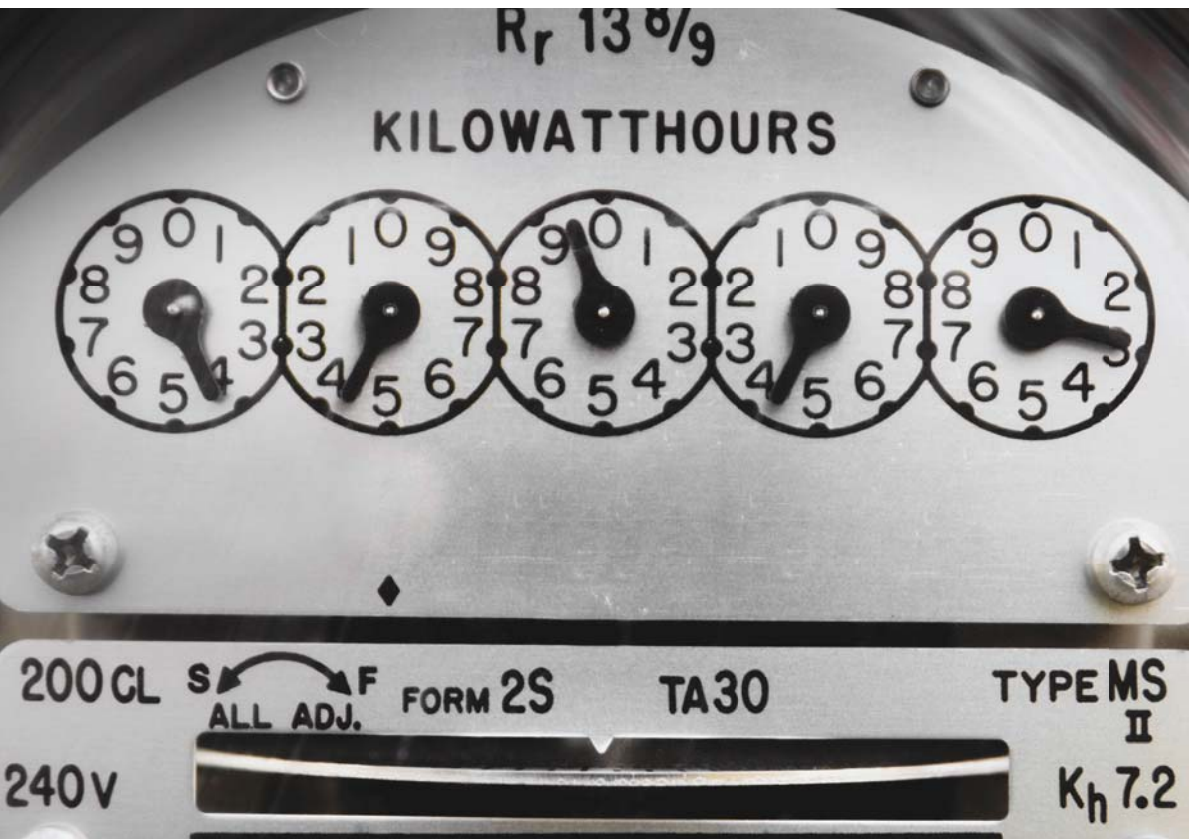
If you're a creditor or financial institution with covered accounts, you must develop and implement a written Identity Theft Prevention Program. The Program must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones. 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**



1 IDENTIFY RELEVANT

What are “red flags”? They’re the signs or specific activities indicating potential risk. Although there’s no one-size-fits-all

Risk Factors Different types of risk. For example, red flags for credit accounts differ from red flags for credit cards. And red flags for consumer accounts may not be the same as red flags for business accounts. And red flags for accounts opened in person may differ from red flags for accounts opened by phone. Therefore, in identifying the relevant red flags for the accounts you offer or maintain, consider the types of accounts covered; how you provide services; and what you have learned about identity theft.

Sources of Red Flags Consider the sources of information, including how identity theft has changed in your business and the experience of your customers. Because technology and criminal activity are constantly changing, keep up-to-date on new threats.

Categories of Common Red Flags The Red Flags Rule lists five specific categories of red flags to consider including in your Program. Some red flags are only relevant to your business or organization when combined or considered in context with other red flags, such as identity theft. The examples, list of red flags is an exhaustive compilation or a list of red flags is a way to help think about relevant red flags for your business.



1. Alerts, Notifications, and Credit Reporting Comp

Here are some examples of consumer's credit activity th

- a fraud or active duty alert
- a notice of credit freeze in report
- a notice of address discrepancy reporting agency
- a credit report indicating with the person's history volume of inquiries or th accounts; an unusual num relationships; or an accou abuse of account privileg

2. Suspicious Documents

Sometimes paperwork has t Here are examples of red fla

- identification that looks
- the person presenting the the photo or match the p
- information on the ident the person presenting the doesn't match with other or recent check
- an application that looks 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,¹¹ or a number that hasn't been issued, according to the monthly issuance tables available from the Social Security Administration¹²
- 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 A

Sometimes the tip-off is ho
some red flags related to ac

- soon after you're notified
for new or additional c
users to the account
- a new account that's us
example, the customer
makes only an initial p
is used for cash advanc
merchandise easily con
- an account that's used i
patterns – for example,
of missed payments, a l
credit, a major change
electronic fund transfe
patterns for a cell phon
- an account that's been
used again
- mail sent to the custom
undeliverable although
on the account
- information that the cu
statements in the mail
- information about una

5. Notice from Other Sou

Sometimes a red flag that a
fraudulently can come from
a law enforcement authorit

2 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, reasons for a name, address, and identification verification, checking a current document like a driver's license or passport you may want to compare that you can find out from other sources or data broker, the Social Security number, or publicly available information.¹ Relying on information from other sources to verify someone's identity.

Existing accounts To detect changes in your Program may include re-verify existing customers (confirming that they are your customer), monitor transactions, change-of-address requests. For Federal Financial Institutions, multi-factor authentication as a starting point, including using passwords, PINs, or biometric identification. Certain information like a Social Security number, or mailing address – are not generally easily accessible.

You may already be using programs that indicate the possibility of behavior that indicates the possibility to validate changes of address. If that information is added into your Program.

3 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.

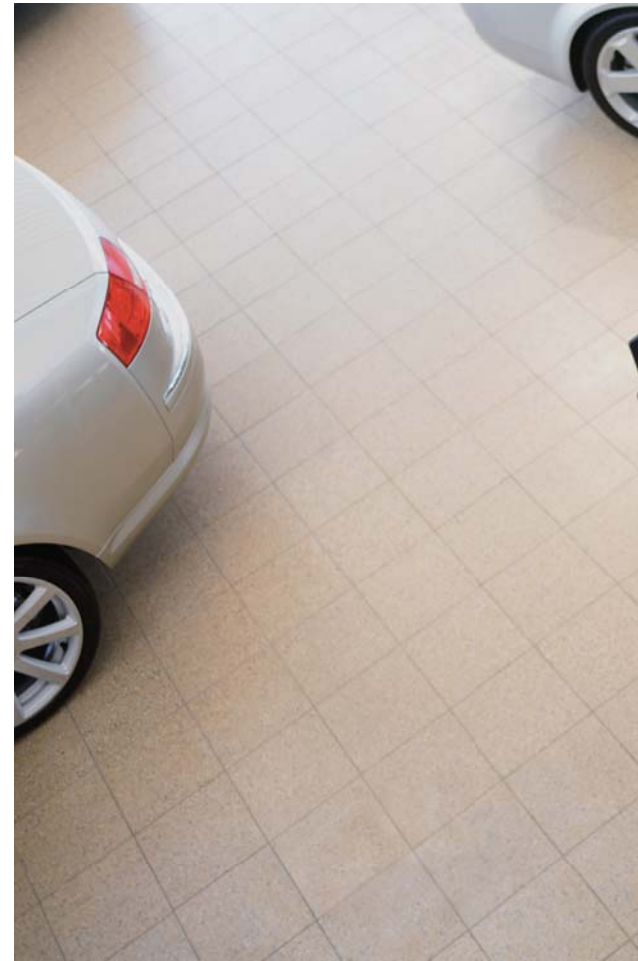
The Guidelines in the Red Flags Rule offer examples of some appropriate responses, including:

- 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.

4 UPDATE THE PR

The Rule recognizes that new red flags or identity thieves change their tactics. Updates to your Program to ensure you address theft risks. Factor in your own changes in how identity thieves operate; changes to mitigate identity theft; changes in your business, such as mergers, acquisitions, ventures, and arrangements with



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 whether your organization is complying with the Rule, and making changes to your Program.

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

In administering your Program, you should consider service providers. If they're conducting activities, for example, opening or managing accounts, providing customer service, or collecting information, you should set standards you would if you were doing it yourself. One way to make sure your service providers are doing it is to add a provision to your contract that requires them to place to detect red flags and either report them or act appropriately to prevent or mitigate them. Other ways to monitor them include reviewing their red flags policies, reviewing their red flags they have detected and

It's likely that service providers will be required to report to client companies. As a result, there will be more service providers that have their own red flags policies. The requirements of the Rule.

The person responsible for your Program should report to the board of directors or a designated committee. They should evaluate how effective your Program is in reducing the risk of identity theft; how you are working with service providers; significant incidents; your 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

ftc.gov/os/fedreg/2007/november/071109redflags.pdf

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/idtheft/bus69.pdf

Information Security Interactive Video Tutorial

ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html

**Questions?
Contact the Red
Contact**

ENDNOTES

1. The Red Flags Rule was promulgated in 2007 pursuant to 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. § 681.2. See also 72 Fed. Reg. at 63,772 (Nov. 9, 2007). You can find the full text at www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. The preamble – pages 63718-63733 – discusses the purpose, intent, and scope of coverage of the Rule. The text of the FTC Rule is at pages 63772-63774. The Rule includes Guidelines – Appendix A, pages 63773-63774 – that are intended to help businesses develop and maintain a compliant Program. The Supplement to the Guidelines – page 63774 – provides a list of 26 examples of red flags for businesses and organizations to consider incorporating into their Programs. This guide does not address companies’ obligations under the Address Discrepancy Rule or the Card Issuer Rule, also contained in the Federal Register with the Red Flags Rule.
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. § 681.2(b)(9).
4. See 15 U.S.C. § 1691a(f). See also 15 U.S.C. § 1681a(b).
5. The Rule’s definition of “financial institution” is found in the FCRA. See 15 U.S.C. § 1681a(t). 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 ECOA, 15 U.S.C. § 1691a. The ECOA defines “credit” as a loan to a debtor to defer payment of debt or to purchase property or services under 1691a(d). The ECOA defines “credit” as “renews or continues credit; any payment, renewal, or continuation of credit by a creditor who participates in the decision to extend, renew, or continue credit.” 15 U.S.C. § 1691a(e). The term “person” includes “any government or governmental subdivision, agency, or cooperative, or association.” 15 U.S.C. § 1691a(f). See 72 Fed. Reg. 13161 (Mar. 18, 2007).
7. An “account” is a continuing relationship between a financial institution or creditor to an individual, family, household, or business pursuant to which the institution or creditor does not include a one-time transaction with a customer, such as a withdrawal from an account.
8. See 16 C.F.R. § 681.2(b)(3)(i).
9. 16 C.F.R. § 681.2(b)(3)(ii).
10. See 16 C.F.R. § 681.2(b)(9).
11. The Social Security Administration can buy that contains records of Federal Reserve Security Administration. See www.ssa.gov.
12. See www.ssa.gov/employer/ssnv.
13. These verification procedures are applicable to the Program Rule applicable to bank accounts. The Rule may be a helpful starting point.
14. “Authentication in an Internet Banking System” is available at www.ffiec.gov/press/p.
15. See 72 Fed. Reg. at 63,773.



FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)
ftc.gov/redflagsrule

March 2009

