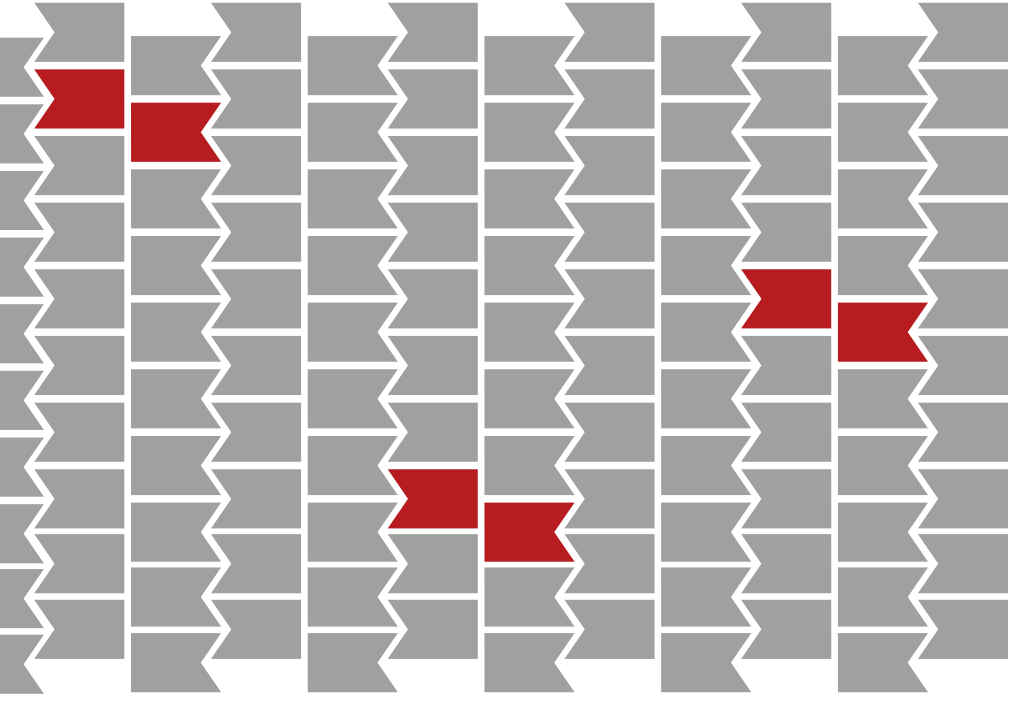
Federal Trade Commission
Protecting America's Consumers

FTC BUSINESS CENTER
YOUR LINK TO THE LAW

FIGHTING FRAUD WITH THE RED FLAGS RULE

A How-To Guide for Business



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

FIGHTING FRAUD WITH THE RED FLAGS RULE

A How-To Guide for Business

As many as nine million Americans have their identities stolen each year. Identity thieves may drain their accounts, damage their credit, and even endanger their medical treatment. The cost to businesses – left with unpaid bills racked up by scam artists – can be staggering, too.

The "Red Flags" Rule, in effect since January 1, 2008, requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or "red flags" – of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts.[1] By identifying red flags in advance, they will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into a costly episode of identity theft.

The Red Flags Rule is enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration. If you work for a bank, federally chartered credit union, or savings and loan, check with your federal regulatory agency for guidance. Otherwise, this booklet has tips for determining if you are covered by the Rule and guidance for designing your Identity Theft Prevention Program.

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 also must include appropriate staff training. If you outsource or subcontract parts of your operations that would be covered by the Rule, your Program also must address how you'll monitor your contractors' compliance.

The Red Flags Rule 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 that addresses a high risk of identity theft in a complex organization, others with a low risk of identity theft could have a more streamlined Program.

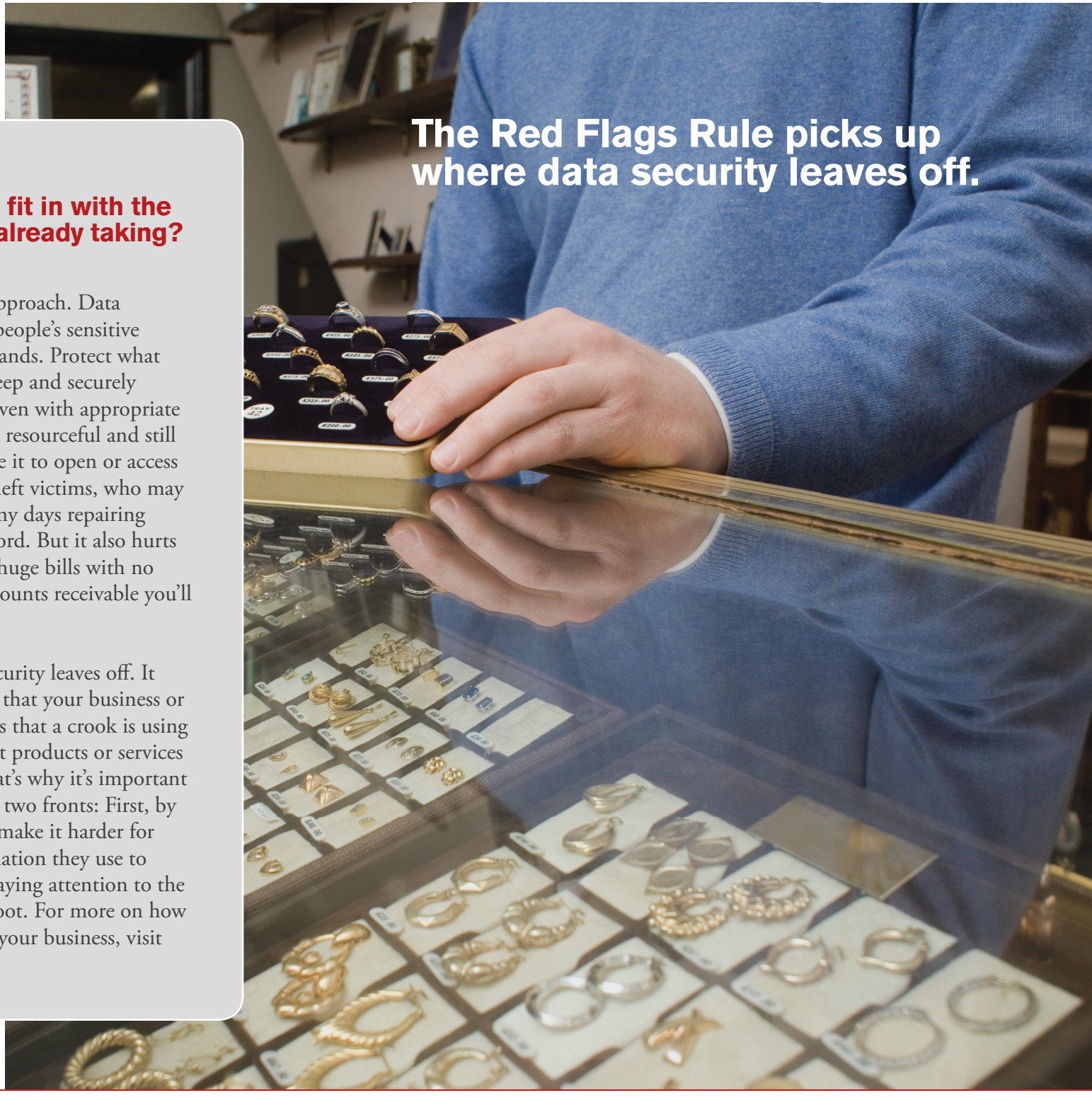
QUESTION:

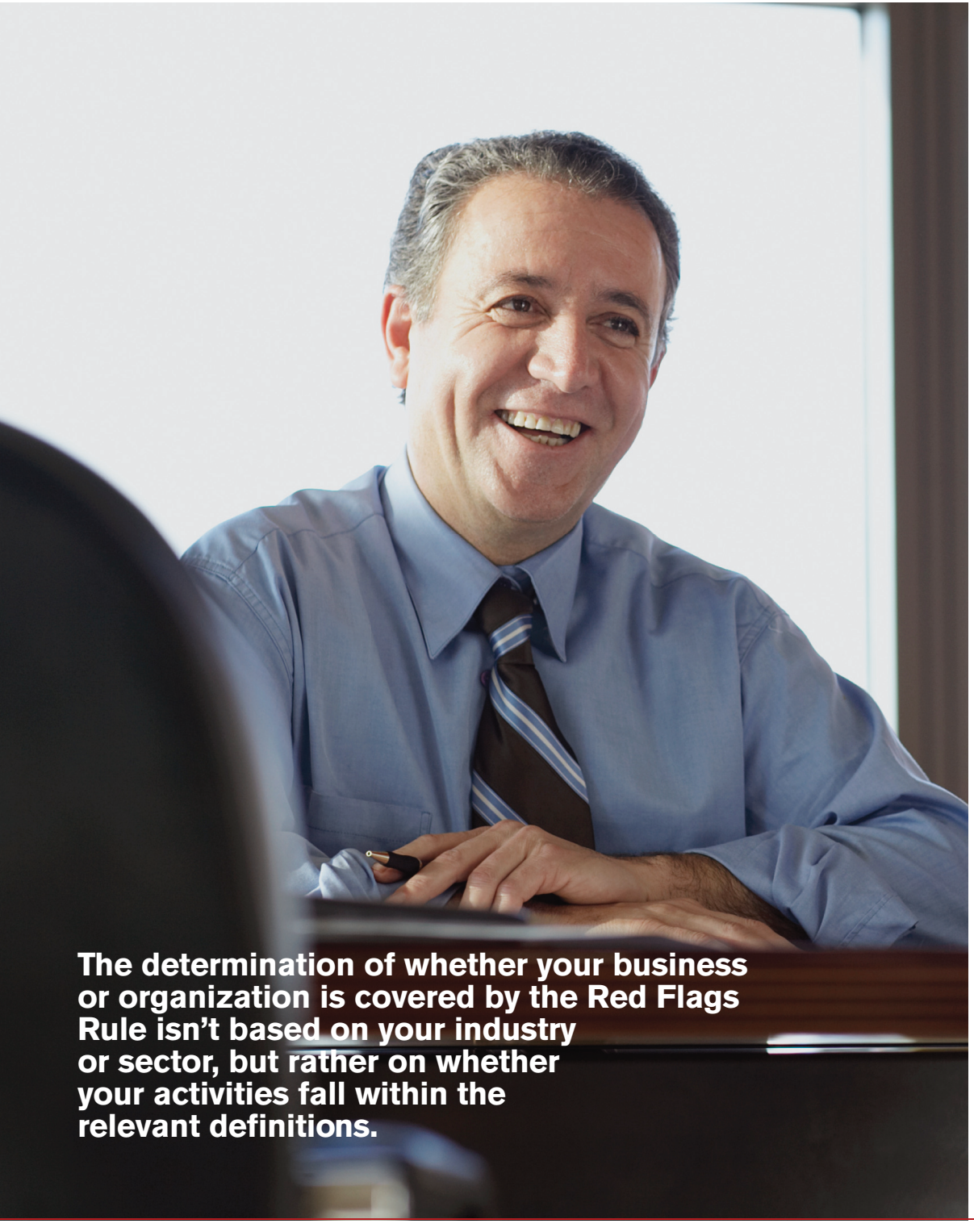
How does the Red Flags Rule fit in with the data security measures we're already taking?

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 "financial institutions" and "creditors." The Rule requires you to conduct a periodic risk assessment to determine if you have "covered accounts." You need to implement a written program only if you have covered accounts.

It's important to look closely at how the Rule defines "financial institution" and "creditor" because the terms apply to groups that might not typically use those words to describe themselves. For example, many non-profit groups and government agencies are "creditors" under the Rule.[4] 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 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 any other person that, directly or indirectly, holds a transaction account belonging to a consumer.[5] Banks, federally chartered credit unions, and savings and loan associations come under the jurisdiction of the federal bank regulatory agencies and/or the National Credit Union Administration. Check with those agencies for guidance tailored to those businesses. The remaining financial institutions come under the jurisdiction of the FTC. Examples of financial institutions under the FTC's jurisdiction are state-chartered credit unions, mutual funds that offer accounts with check-writing privileges, or other institutions that offer accounts where the consumer can make payments or transfers to third parties.

Creditor The definition of "creditor" is broad and includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later.[6] Utility companies, health care providers, and telecommunications companies are among the entities that may fall within this

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 account" is "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."[9] 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 permit multiple payments or transactions – they always are "covered accounts" under the Rule – other types of accounts are "covered accounts" 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 – such as through the Internet or by telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these.

?

QUESTION:

I know our company is a "creditor" under the Rule because we issue credit cards. But we also have non-credit accounts. Do we have to determine if both types of accounts are "covered accounts?"

ANSWER:

Yes, and the same goes for financial institutions with transaction and non-transaction accounts. For example, a telecommunications company that has accounts that are billed after service is rendered (credit accounts) and accounts that are prepaid or paid when service is rendered (non-credit accounts) would have to evaluate both types of accounts to determine if they're covered. Likewise, a broker-dealer that offers accounts with check-writing privileges (transaction accounts) and without those privileges (non-transaction accounts) would have to consider both kinds of accounts to determine if they're 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.

step 4

Update your Program.

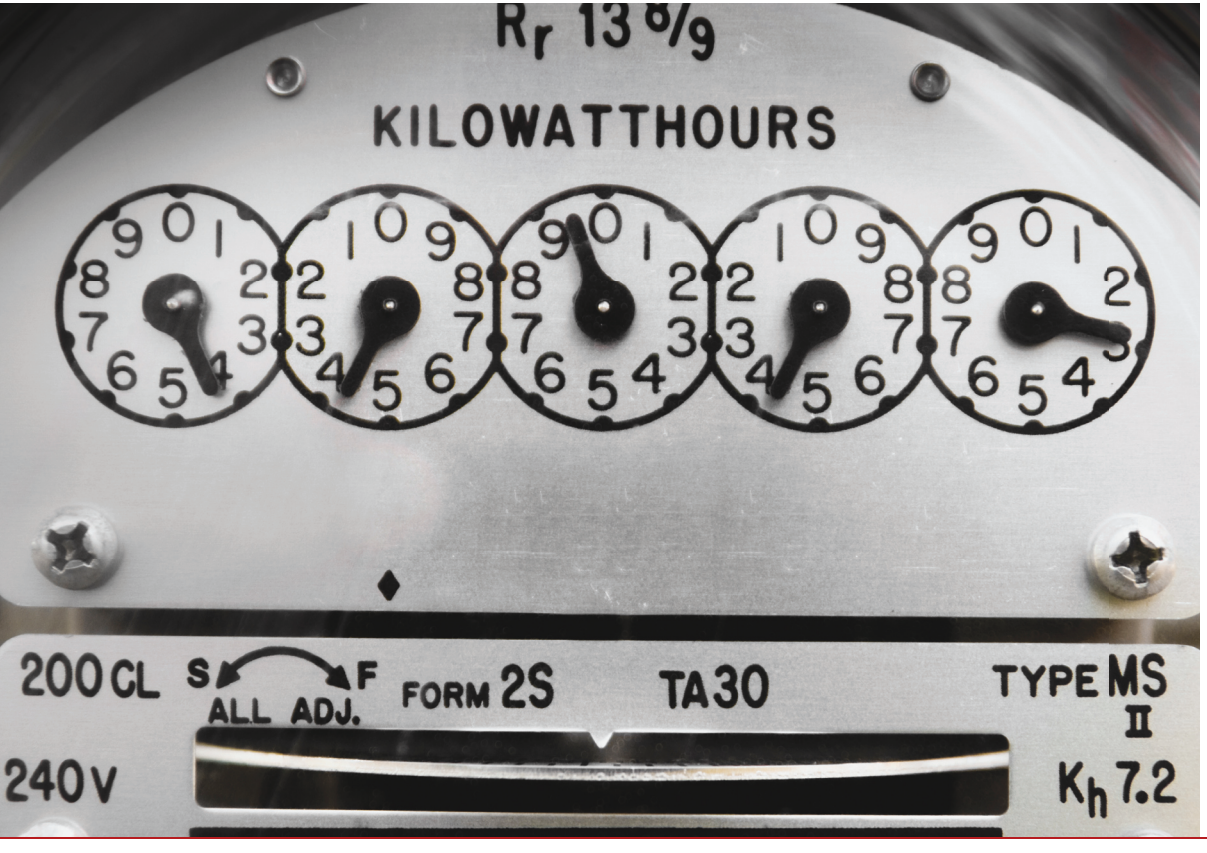
The risks of identity theft can change rapidly, so it's important to keep your Program current and educate your staff.

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 RED FLAGS

What are "red flags"? They're the potential patterns, practices, or specific activities indicating the possibility of identity theft.[10] Although there's no one-size-fits-all approach, 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. Similarly, the red flags for consumer accounts may not be the same as those for business accounts. And red flags for accounts opened or accessed online or by phone may differ from those involving face-to-face contact. Therefore, in identifying the relevant red flags, consider the types of accounts you offer or maintain; the methods used to open covered accounts; how you provide access to those accounts; and what you have learned about identity theft in your business.

Sources of Red Flags Consider other sources of information, including how identity theft may have affected your business and the experience of other members of your industry. Because technology and criminal techniques change constantly, keep up-to-date on new threats.

Categories of Common Red Flags Supplement A to the Red Flags Rule lists five specific categories of warning signs to consider including in your Program. Some examples may be relevant to your business or organization. Some may be relevant only when combined or considered with other indicators of identity theft. The examples, listed on the following pages, aren't an exhaustive compilation or a mandatory checklist, but rather a way to help think about relevant red flags in the context of your business.

1. Alerts, Notifications, and Warnings from a Credit Reporting Company.

Here are some examples of changes in a credit report or a consumer's credit activity that may 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 agency
- a credit report indicating a pattern of activity inconsistent with the person's history – for example, a big 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

2. Suspicious Documents.

Sometimes paperwork has the telltale signs of identity theft. Here are examples of red flags involving documents:

- identification that looks altered or forged
- the person presenting the identification doesn't look like the photo or match the physical description
- information on the identification that differs from what the person presenting the identification is telling you or doesn't match with other information, like a signature card or recent check
- an application that looks like it's been altered, forged, 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,[11] or a number that hasn't been issued, according to the monthly issuance tables available from the Social Security Administration[12]
- 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 the account is being used. Here are some red flags related to account activity:

- soon after you're notified of a change of address, you're asked for new or additional credit cards, cell phones, etc., or to add users to the account
- a new account that's 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 that's used in a way inconsistent with established patterns – for example, nonpayment when there's no history of missed payments, a big increase in the use of available credit, a major change in buying or spending patterns or electronic fund transfers, or a noticeable change in calling patterns for a cell phone account
- an account that's been inactive for a long time is suddenly used again
- mail sent to the customer that's returned repeatedly as undeliverable although transactions continue to be conducted on the account
- information that the customer isn't receiving their account statements in the mail
- information about unauthorized charges on the account

5. Notice from Other Sources.

Sometimes a red flag that an account has been opened or used fraudulently can come from a customer, a victim of identity theft, a law enforcement authority, or someone else.

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 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 information with the information you can find out from other sources, like a credit reporting company or data broker, the Social Security Number Death Master File, or publicly available information.[13] Asking challenge questions based on information from other sources can be another way of verifying someone's identity.

Existing accounts To detect red flags for existing accounts, your Program may include reasonable procedures to authenticate customers (confirming that the person you're dealing with really is your customer), monitor transactions, and 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.[14] It explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PIN numbers, 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 good authenticators because they're so easily accessible.

You may already be using programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. If that's the case, 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 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 PROGRAM

The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics. Therefore, it requires periodic updates to your Program to ensure that it keeps current with identity theft risks. 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, such as mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

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 staff reports about how your organization is complying with the Rule, and approving important changes to your Program.

The Rule requires that you train relevant staff only as "necessary" – for example, staff that has received anti-fraud prevention training may not need to be re-trained. Remember though, 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 themselves. Other ways to monitor them include giving them a copy of your Program, reviewing their red flags 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 using service providers that have 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 the 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.[15]

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 about complying with the Red Flags Rule?

Contact RedFlags@ftc.gov

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 also15 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 others. Transaction accounts include checking accounts, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.
6. "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. 13161 (Mar. 18, 2003).
7. 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. § 681.2(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.
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 Death Master File is a service companies can buy that contains records of deaths that have been reported to the Social Security Administration. See www.ntis.gov/products/ssa-dmf.aspx.
12. See www.ssa.gov/employer/ssnvhighgroup.htm.
13. These verification procedures are set forth in the Customer Identification Program Rule applicable to banking institutions, 31 C.F.R. § 103.121. This Rule may be a helpful starting point in developing your Program.
14. "Authentication in an Internet Banking Environment" (Oct. 12, 2005), available at www.ffiec.gov/press/pr101205.htm.
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