The Red Flags Rule: Frequently Asked Questions

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations. The staff of the Federal Trade Commission (FTC) has heard from companies across the country that are developing Programs. Their questions — and the FTC's answers — may help you develop a Program for your business.

These FAQs relate only to the Red Flags Rule and don't address the applicability of other laws. If you work for a bank, federally chartered credit union, or savings and loan, check with your federal regulatory agency for guidance. The FAQs represent the opinions of the FTC staff, and aren't binding on the Commission.Â FTC staff will update these FAQs to address new questions from businesses.

A. General Questions About the Red Flags Rule

B. Who's Covered by the Red Flags Rule?

C. The Red Flags Rule and Government Agencies, Non-Profit Organizations, and Schools

D. Designing Your Identity Theft Prevention Program

E. Red Flags Rule Compliance and Enforcement

A. General Questions About the Red Flags Rule

1. Where can I find the Red Flags Rule?

   The Red Flags Rule is on the FTC's website:www.ftc.gov/redflagsrule orwww.ftc.gov/os/fedreg/2007/november/071109redflags.pdf.1The text of the Rule is on page 63772, but you may want to read several other parts. The Preamble — beginning on page 63718 — explains the rationale behind the Rule and what it covers. The Guidelines — beginning on page 63773 — list issues to think about in developing your Identity Theft Prevention Program. The Supplement to the Guidelines — page 63774 — gives 26 possible red flags to consider.

2. I'm not an attorney. Where can I find plain-language guidance on complying with the Rule?

   The FTC has published a booklet,*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, with advice on complying with the Rule. In addition, the FTC has created aform with step-by-step instructions on designing a Program for businesses and organizations at low risk for identity theft. There also are short articles on Red Flags compliance for your newsletter or website. Find these resources — and more — atwww.ftc.gov/redflagsrule.

B. Who's Covered by the Red Flags Rule?

1. What types of businesses and organizations are covered by the Red Flags Rule?

   The Rule applies to "financial institutions" and "creditors." It's important to look closely at how the Rule defines those terms because they apply to groups that might not typically use those words to describe themselves. Whether your business or organization is a financial institution or creditor isn't based on the line of work you're in, but rather on whether your activities fall within the definitions in the law. The Red Flags Rule gives examples of businesses and organizations that probably are covered, but the list isn't exhaustive.

   The Rule defines a "financial institution" as: 1) a state or national bank, 2) a state or federal savings and loan association, 3) a mutual savings bank, 4) a state or federal credit union, or 5) any other entity that directly or indirectly holds a "transaction account" belonging to a consumer.2"Transaction accounts" are deposits or accounts from which a consumer can make payments or transfers to third parties.3 Banks, federally chartered credit unions, and savings and loans come under the jurisdiction of the federal bank regulatory agencies or the National Credit Union Administration and should check with

them for guidance. The FTC's jurisdiction extends to state chartered credit unions and other institutions that hold transaction accounts — for example, mutual funds that offer accounts with check writing or debit card privileges or other businesses that offer accounts where consumers can make payments or transfers to third parties.

Under the Rule, the definition of "creditor" is broad, and includes businesses or organizations that regularly provide goods or services first and allow customers to pay later.4Examples of groups that may fall within this definition are utilities, health care providers, lawyers, accountants, and other professionals, and telecommunications companies. The definition also covers businesses or organizations that regularly grant loans, arrange for loans or the extension of credit, or make credit decisions. Examples include finance companies, mortgage brokers, and automobile dealers or retailers that offer financing or collect or process credit applications for third party lenders. 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 would be a creditor under the Rule.

For more on the definitions of "financial institution" and "creditor," read*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, atwww.ftc.gov/redflagsrule.

2. Do all creditors and financial institutions need to have a written Identity Theft Prevention Program?

   Only creditors and financial institutions that have "covered accounts" need a Program. Once you've determined you're a creditor or financial institution under the Red Flags Rule, the next step is to figure out if you have any covered accounts. The Rule defines that term as either: 1) consumer accounts designed to permit multiple payments or transactions, or 2) any other account that presents a reasonably foreseeable risk from identity theft.

   If you have covered accounts, you must develop and implement a written Program to detect and respond to the red flags of identity theft — taking into consideration the nature of your business and the risks you face — and update your Program periodically. If you don't have any covered accounts, you don't need a written Program, but you still need to conduct periodic risk assessments to determine if you've acquired any covered accounts through changes to your business.

   For more about covered accounts, read*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, atwww.ftc.gov/redflagsrule.

3. Is my coverage under the Red Flags Rule based on whether I pull credit reports or collect personal information like Social Security Numbers?

   No. Coverage under the Rule is based on whether your activities fall within the definitions of "financial institution" or "creditor." Even if you don't pull credit reports or

collect personal information, you're covered by the Rule if your activities meet the definitions of "financial institution" or "creditor" — for example, deferring payment for goods or services. See Question B.1. for more on who's covered by the Rule.

4. Am I a creditor because I accept certain forms of payment — say, checks, credit or debit cards, or automatic account debits — even if I don't extend or arrange for credit myself?

   Merely accepting credit cards or other forms of payment doesn't make you a creditor under the Red Flags Rule. Coverage as a creditor is based on whether your activities meet the definitions in the law.

5. Our clients pay a retainer before we provide services. Although we may send an invoice for our charges, we satisfy it by drawing on the retainer. Does this make us a creditor under the Red Flags Rule?

   No, an arrangement like that wouldn't make your business a creditor. Many businesses require a payment before work begins. For example, a law firm may require clients to pay a retainer. Some medical practices charge patients monthly fixed fees for unlimited services. They may send their clients or patients invoices each month, but draw payment from the money they've already received. The Red Flags Rule applies to businesses that regularly defer payment until*after* services have been performed. Because the law firm or medical practice in this example is paid*before* they provide services, these arrangements aren't "credit," as the law defines that word.

6. My law firm brings cases on a contingency basis. Does this type of fee arrangement make me a creditor under the Red Flags Rule?

   No. Generally, under a contingency fee arrangement, a law firm will not earn its fee unless and until it wins a recovery for its client. Therefore, this arrangement is not a credit relationship, and the law firm would not be a creditor under the Red Flags Rule. If, however, the client is responsible for certain litigation expenses regardless of the outcome of the case, the firm would have to consider whether there is a deferral of payment that would meet the definition of "credit."

7. What does it mean to "regularly" extend credit?

   There's no bright line definition for "regularly." But if the activities that meet the definition of "creditor" are more than just an isolated occurrence for your business, the Red Flags Rule applies to you.

8. Am I a creditor under the Rule if I extend credit to other businesses?

   Yes, you're a creditor whether you have consumer or business customers.

9. Do I have covered accounts if I'm a business creditor?

It depends. If you're a creditor with only business-to-business accounts, you have to assess whether those accounts pose a reasonably foreseeable risk from identity theft. If they do, they're "covered accounts" under the Rule.

10. Am I a creditor if I regularly refer customers to third parties for credit?

    It depends. A "creditor" includes any person who "regularly arranges for the extension, renewal, or continuation of credit."5For example, mortgage brokers, auto dealers, or retailers that regularly collect or process credit applications for third-party lenders are creditors under the Rule. You're not a creditor if you merely provide advertising brochures for third-party financing or tell your customers about third-party financing without referring them to lenders.

11. I regularly arrange for the extension, renewal, or continuation of credit for my customers, so I've determined I'm a "creditor" under the Red Flags Rule. Do I need to have a written Identity Theft Prevention Program?

    You do, if you have "covered accounts." Under the Red Flags Rule, "covered accounts" are: 1) consumer accounts that permit multiple payments or transactions, or 2) any other accounts for which there is a reasonably foreseeable risk from identity theft. For example, a retailer that can process a credit or payment transaction in the store on the customer's store-branded account without using the actual card or account number will likely have consumer accounts that permit multiple payments or transactions. Other businesses — say, a car dealer that has only a single transaction with a customer they refer for third-party financing — need to consider if they fall within the second part of the definition: an account for which there is a reasonably foreseeable risk from identity theft. Likewise, a company that refers other businesses for credit would need to consider whether there is a reasonably foreseeable risk from identity theft arising from the transaction. For more on "covered accounts," read*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, atwww.ftc.gov/redflagsrule. For more on what your Program might look like, see Question D.9.

12. Our company offers individual retirement plans that allow participants to get loans from their own plan account. Does that make us or the plan a creditor under the Rule?

    When participants in an individual retirement plan — say, a 401(k) plan — get loans, they're generally borrowing from their own funds. Just allowing participants to borrow from their funds would not — by itself — make the plan sponsor or the plan a "creditor" under the Rule.

13. If our company meets the definition of a "financial institution" or "creditor," are the individual retirement accounts we make available to our employees considered "covered accounts" that must be included in our written Identity Theft Prevention Program?

    Individual retirement accounts generally qualify as "covered accounts."6However, in certain cases — for example, 401(k) plans — the account that a participant establishes

isn't with the employer or plan sponsor. Instead, the participant establishes an account with the plan itself, which is a separate legal entity. Under those circumstances, the employer would not need to include the retirement plan accounts in a written Identity Theft Prevention Program.

14. Am I a creditor if I offer my employees health care flexible spending accounts that reimburse them for elected amounts that are more than they've contributed to date? Am I a creditor if I serve as a third-party administrator that maintains those accounts for employees of other companies?

    No. Health care flexible spending accounts operate like insurance plans in that employers must make the entire amount elected by participants available to them from the beginning of the plan year. If they leave your company before the end of the plan year, they aren't required to make up any difference between the amount they contributed and the benefits they received. As a result, neither offering your employees health care flexible spending accounts nor maintaining those accounts for other companies makes your business a "creditor" under the Rule.

15. Are we a "financial institution" under the Red Flags Rule if we have accounts for our clients and offer a way for them to make payments or transfers to third parties with a debit card, check, or wire transfer?

    Yes. The definition of "financial institution" includes businesses that have accounts a customer can use to make payments or transfers to third parties. For example, a university may hold student funds in an account and give students a card they can use to make purchases at local stores. This type of arrangement would make the university a financial institution under the Rule. If you provide government benefits or administer flexible spending accounts and give your customers a debit card to access benefits, you would be considered a financial institution.

C. The Red Flags Rule and Government Agencies, Non-Profit Organizations, and Schools

1. Does the Red Flags Rule apply to government agencies and non-profit organizations?

   Yes. If the activities of the government agency or non-profit organization fall within the statutory definitions of "financial institution" or "creditor," they're covered by the Rule.7For example, cities that operate utilities that regularly bill customers after they've received services or colleges that regularly provide student loans or process student loan applications are creditors under the Rule. For more on whether the Red Flags Rule applies to your agency or organization, see Question B.1. and B.15.

2. What about municipalities, cities, or counties that send tax bills, issue parking tickets, or impose fines? Are they "creditors" under the Rule?

   No. Financial obligations like that are not considered "credit" for purposes of the Red Flags Rule. In this context, "credit" assumes an underlying transaction that a customer enters into voluntarily. Taxes, fines, and the like don't fit that definition.

3. What if I work for a municipality, city, or county, and we've already determined our activities fall within the Rule's definition of "creditor" or "financial institution"? Do our taxes, fines, etc., become "covered accounts" under the Red Flags Rule?

   No. These fees are not covered accounts under the Rule because a person is not establishing a relationship to get goods or services.8

4. If we provide a mandatory municipal service that a customer can't decline — like sewage — are we considered a "creditor" under the Rule?

   It depends. Generally, there are two types of billing arrangements for mandatory services. As explained in Question C.2., if you bill customers a flat fee, it's like a tax and you wouldn't be a creditor under the Rule. If you charge customers based on how much they use and then send them a bill, it's more like a utility transaction and you would be a creditor.

5. Are schools that regularly offer tuition payment plans creditors under the Rule?

   It depends on how they structure the plans. Schools that bill for tuition after students attend class are creditors. Schools that require payment upfront or "pay as you go" — so that students could be barred from class if they don't pay — are not creditors.

D. Designing Your Identity Theft Prevention Program

1. Do creditors or financial institutions have to develop an Identity Theft Prevention Program if they already comply with data security requirements like the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLB)?

   Yes. The FTC strongly encourages reasonable data security practices, but the Red Flags Rule is not a data security regulation. Good data security practices — like collecting only the personal information you need, protecting that information, and securely disposing of what you no longer need — help ensure that personal information does not fall into the hands of identity thieves. For more on data security, visitwww.ftc.gov/infosecurity.

   Â The Red Flags Rule picks up where data security leaves off. If identity thieves*do*get hold of someone's personal information, they typically use it to get goods or services from unsuspecting businesses and have no intention of paying the bill. By having

companies set up procedures to look for and respond to the "red flags" that an identity thief is trying to use someone else's information, the Rule seeks to reduce the damage crooks can inflict both on victims of identity theftand on businesses left with accounts receivable they'll never be able to collect. While you may be able to incorporate some of your data security practices, your Identity Theft Prevention Program is a different kind of plan aimed at preventing a different kind of harm.

2. Does the Rule require that I have specific practices or procedures in my Program — like identifying a particular red flag or reporting suspected identity theft?

   The Rule doesn't require any specific practice or procedures. It gives you the flexibility to tailor your Program to the nature of your business and the risks it faces. The FTC will assess compliance based on the reasonableness of a company's policies and procedures. Businesses with a high risk for identity theft may need more robust procedures — like using other information sources to confirm the identity of new customers or incorporating fraud detection software. Groups with a low risk for identity theft may have a more streamlined Program — for example, simply having a plan for how they'll respond if they find out there has been an incident of identity theft involving their business. The FTC has designed aform to help groups at low risk for identity theft put together a Program. It's available atwww.ftc.gov/redflagsrule.

3. Does the Red Flags Rule require me to check photo IDs of my customers? If I check photo IDs, should I keep copies?

   The Rule doesn't specifically require you to check customers' photo IDs. Of course, for some businesses, checking photo IDs is one way to verify that customers are who they claim to be. But if you decide to ask for a photo ID, keeping a copy often is unnecessary and can raise privacy and data security concerns, especially if you're collecting other personal information like date of birth, address, or Social Security number.

4. Does the Red Flags Rule require that I use Social Security numbers to verify my customers' identity?

   No, the Red Flags Rule does not require that you use Social Security numbers or any other specific identifying information. Whether you collect Social Security numbers or other information to verify a customer's identity depends on the nature of your business and the risks you face. Actually, collecting a Social Security number by itself is not a reliable way to verify someone's identity because the numbers are widely available and do not prove a person is who he or she claims to be. However, Social Security numbers can be helpful as part of a more comprehensive identity verification process — for example, as a way to check against information from other sources or as a way to get other information, like a credit report, which can be used to verify a person's identity.

   It's a good data security practice not to collect more information than you need. If you are asking for a Social Security number, but not actually using it as part of a more

comprehensive authentication process, reconsider whether your business really needs to collect and maintain it.

5. How do my obligations under other laws affect the implementation of my Identity Theft Prevention Program?

   Your Program under the Red Flags Rule should be consistent with other relevant legal, professional, and ethical obligations. This would include laws relating to the provision of medical treatment or the provision and termination of utility services. Indeed, the Rule anticipates the need to accommodate obligations like these by requiring that a Program include only "reasonable" policies and procedures, and by ensuring that each group has the flexibility to tailor a Program to the nature of its business.

6. Under what circumstances should I contact law enforcement? Who handles identity theft?

   If your business or organization experiences a confirmed incident of identity theft, it's a good idea to report it to law enforcement. Your local police department would be a good place to start. If you suspect your business is being targeted specifically — say, by a persistent attack on your website — consider contacting the FBI or U.S. Secret Service. The FTC does not have jurisdiction to prosecute identity thieves, but it has many resources to help victims recover. Consider directing victims to the FTC's identity theft website,www.ftc.gov/idtheft.

7. Are there samples or templates to help me set up my Program?

   Yes. The FTC has created aform to help businesses at low risk for identity theft design a Program. It's atwww.ftc.gov/redflagsrule. Many trade associations have developed guidance to help industry members comply with the Rule, too. The FTC cannot recommend any particular vendor's compliance products or services.

8. Is there a Red Flags certification or accreditation that will ensure our Program complies with the Rule?

   No. Some companies and organizations offer Red Flags compliance services, but the FTC doesn't certify or approve any particular program. It's up to you to decide if you need help like that. Before paying for Red Flags compliance services, visitwww.ftc.gov/redflagsrule for free resources developed by the FTC to help you design your Program.

9. We're a creditor that regularly arranges for our customers to get credit from third partiesand we have covered accounts. What should our Identity Theft Prevention Program look like?

   You can create your own policies and procedures for your Program or incorporate reasonable policies and procedures from the lender's Program. Reasonable procedures might include asking for photo identification, comparing the photo to the person presenting the ID, looking for signs the ID has been altered or forged, and comparing the

information on the ID with what's on the credit application. Your Program also should include reasonable procedures for responding to red flags and complying with the Rule's administrative requirements.

10. Does the FTC have a sample training policy for employees?

    No. That wouldn't be practical because each Program is unique. Your employee training policies should be based on the specific red flags you've identified in your business or organization and the procedures you've put in place for detecting and responding to those red flags.

11. What if we hire service providers? If our business has to have a Program under the Rule, do our service providers need a Program, too?

    It depends on what they're doing for your business. There are generally two types of service providers you'll need to supervise under the Rule. First, there are service providers in the business of fraud detection who help identify, detect, and respond to red flags. If you hire a company like that, you must make sure it's meeting the same standards that would apply if you were doing those things yourself.

    Second, other companies you hire may not be in the business of fraud detection, but will be the only ones who can detect the red flags you've identified in your Program. For example, a debt collector you use to contact customers about outstanding debts may hear from consumers who have been the victims of identity theft. Certainly, if you were performing that task yourself, you'd spot that as a red flag. Since you've hired a debt collector, you must ensure that they either comply with your Program or have their own policies and procedures to detect and respond to red flags. Under the Red Flags Rule, you do not need to supervise service providers who merely have access to data about your customers, but aren't in a position to detect the red flags in your Program — like janitorial contractors or certain types of software support providers. For more about service providers, read*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, atwww.ftc.gov/redflagsrule.

E. Red Flags Rule Compliance and Enforcement

1. Can a consumer sue us under the Red Flags Rule?Â

   No, there is no private right of action. Only certain federal and state government agencies can enforce the Rule,9but consumers can file a complaint with the FTC about a company's Program. The FTC uses complaints filed atwww.ftc.gov to target its law enforcement efforts.

2. If my business is covered by the Red Flags Rule, what will we need to show the FTC to prove we're complying? Is there a specific audit document we have to file or have available if asked?

   The FTC does not conduct routine compliance audits. But the FTC can conduct investigations to determine if a business within its jurisdiction has taken appropriate steps to develop and implement a written Program, as required by the Rule. The FTC may ask the target of the investigation to produce copies of its Program and other materials related to compliance. The FTC also may interview officers, employees, or others who are familiar with the company's practices. If the FTC has reason to believe the Rule has been violated, it can bring an enforcement action.

3. I'm a creditor with consumer or household accounts, but I think it's very unlikely that an identity thief will try to defraud me. Do I still have to prepare an Identity Theft Prevention Program?

   The Red Flags Rule requires all creditors with covered accounts to prepare an Identity Theft Prevention Program ("Program"). At the same time, the Commission staff recognizes that your risk of identity theft may be so low that, as a matter of prosecutorial discretion, Commission staff would be unlikely to recommend bringing a law enforcement action under the following circumstances:

   - You know your clients individually. For example, some medical practices and law firms are familiar with everyone who walks into the office. In such circumstances, the likelihood that an identity thief can defraud a business by impersonating someone else is extremely low.
   - Â You provide services to customers in or around their home, such as by operating a lawn care or a home cleaning business. For these types of businesses, the risk of identity theft is extremely low because identity thieves generally do not want people to know where they live.
   - You are involved in a type of business where identity theft is rare. For example, if there are no reports in the news, trade press, or among people in your line of business about identity theft and your business itself has not experienced incidents of identity theft, it is unlikely that identity thieves are targeting your sector.Â

   Of course, from time to time you need to consider whether your identity theft risk has changed, warranting a different approach with respect to the Rule.

4. What are the penalties for noncompliance?

   The FTC can seek both monetary civil penalties and injunctive relief for violations of the Red Flags Rule. Where the complaint seeks civil penalties, the U.S. Department of Justice typically files the lawsuit in federal court, on behalf of the FTC. Currently, the law sets $3,500 as the maximum civil penalty per violation. Each instance in which the company has violated the Rule is a separate violation. Injunctive relief in cases like this often requires the parties being sued to comply with the law in the future, as well as

provide reports, retain documents, and take other steps to ensure compliance with both the Rule and the court order. Failure to comply with the court order could subject the parties to further penalties and injunctive relief.

5. What if I have a question not answered in these FAQs??

   Your question may be answered in our booklet,*Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, our short articles on Red Flags compliance, or ourform with step-by-step instructions on designing a Program for businesses and organizations at low risk for identity theft, all available atwww.ftc.gov/redflagsrule.

---

1 The Red Flags Rule is at 16 C.F.R. Â§ 681.2. It implements section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. Â§ 1681m, which amended the Fair Credit Reporting Act. The FTC recently re-numbered the Identity Theft Red Flags Rule in the Code of Federal Regulations from Â§ 681.2 to Â§ 681.1. For ease of reference, these FAQs use the original numbers.

2 See 15 U.S.C. Â§ 1681a(t).

3 See 15 U.S.C. Â§ 461(b)(1)(C).

4 See 15 U.S.C. Â§ 1681a(r)(5); 15 U.S.C. Â§ 1691a(d); 15 U.S.C. Â§ 1691a(e).

5 See 15 U.S.C. Â§ 1691a(e).

6 This issue was discussed in section II.B.6. of the separate frequently asked questions issued jointly by the FTC, the federal banking agencies, and the National Credit Union Administration (http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf).

7See 15 U.S.C. Â§ 1691a(f) (defining a "person" as "any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity"); 15 U.S.C. Â§ 1681a(b) (defining a "person" as "a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association"); 15 U.S.C. Â§ 1681s(a)(1) (defining FTC jurisdiction under the FCRA).

8 See 16 C.F.R. Â§ 681.2(b)(1).

9 See 15 U.S.C. Â§ 1681m(h)(8).