

The Red Flags Rule: What financial institutions need to know

Grant Thornton LLP Advisory Services

The Red Flags Rule (FTC 16 CFR 681) compliance deadline is fast approaching, and many financial institutions may not be prepared because they do not fully understand the rule's requirements. Furthermore, their existing Red Flags plans may not be as effective as they should be. Whether your institution is far along in the compliance process or just beginning it, this paper will provide you with an overview of the rule, several of the rule's unique features, actions to consider when formulating or assessing your compliance strategy, and a few do's and don'ts to consider.



What is the Red Flags Rule?

The Red Flags Rule is a component of the Fair and Accurate Credit Transactions (FACT) Act signed into law in December 2003. Section 114 of the act required agencies that regulate financial institutions and businesses to jointly develop a set of rules to mandate the detection, prevention and mitigation of identity theft. Collectively, the Federal Trade Commission (FTC), federal bank agencies and the National Credit Union Administration (NCUA) authored a regulation generally known as the Red Flags Rule.

The Red Flags Rule is designed to combat identity theft. The need for this rule is evidenced by the most recent statistics¹ available regarding identity theft in the U.S. In 2008 alone:

- the number of identity fraud victims rose by 22 percent to 9.9 million American adults,
- 7.5 percent of Americans were victims of financial fraud,
- the total annual fraud amount increased to \$48 billion,
- the average fraud amount per incident was \$4,849,
- the average cost to consumers for identity fraud was \$496, and
- at the current pace, one out of every five Americans will have his or her identity stolen this year.

Worse, identity theft has become a global big business favored by organized crime syndicates, terrorist organizations, rogue dictatorships and others with bad intent. Money stolen through identity theft is a significant source of funds for these organizations.

The federal government previously created and enforced a number of rules designed to keep identity thieves from stealing information. However, these regulations didn't address how the stolen information was used **after** it had been stolen. The Red Flags Rule attempts to close the loop on identity theft by making it harder for criminals to use a stolen identity.

¹ "2009 Identity Fraud Survey Report," Javelin Strategy & Research. <http://www.idsafety.net/report.html>

The Red Flags Rule: What financial institutions need to know

Financial institutions: The ultimate targets

The Red Flags Rule is especially geared toward the financial institutions industry. According to the FTC's *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*,² a **financial institution** is defined "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. 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 your business. 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."

A **transaction account** is defined as a deposit or other account from which the owner makes payments or transfers (e.g., checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers and share draft accounts).³

In addition to the types of accounts mentioned above, any other account where there is a "reasonably foreseeable" chance of identity theft is also a covered account. The definition of "reasonably foreseeable" is open to interpretation, but if an account at your institution has a prior history of successful identity theft, that account will likely meet the "reasonably foreseeable" test. In addition, the FTC has stated that accounts with businesses may be covered by the rule – regulation is not limited to consumer-only accounts.

Due to the large numbers of financial institutions and customers, there may be hundreds of different account types that fall into the category of a covered account. As financial information becomes more and more digitized, the number of places where fraud could occur is growing rapidly.

With the increasing use of online banking and the accessibility of personal information on the Web, identity thieves are actively exploiting the gaps in identity theft prevention. The FTC's Red Flags guide lists just some potential signs of wrongdoing, including:

- **Alerts from a credit reporting company.** A fraud or active duty alert, a notice of address discrepancy and a credit report inconsistent with the person's behavior are all potential signals of identity theft.
- **Suspicious personal identifying information.** Red flags include inconsistencies in information (e.g., a date of birth that doesn't match the Social Security Administration's issuance tables), a Social Security number used by another customer to open an account, or a person who omits required application information and doesn't respond to requests for completion.
- **Suspicious account activity.** A long-inactive account that is suddenly used again, a major change in buying or spending patterns, and information that the customer is not receiving his/her statements in the mail are possible indicators of identity theft.

Many financial institutions feel that they already have sufficient controls in place to comply with the Red Flags Rule. However, some have vulnerabilities in the areas of new accounts and account modification. An identity thief will often use a stolen identity to open new accounts or apply for loans. Institutions that open accounts (i.e., credit cards or online bank accounts) over the phone or through mail are especially susceptible. In light of the prevalence of phishing (the practice of sending e-mails that appear legitimate in order to obtain personal information), financial institutions need to ensure they have proper controls in place to validate that the person modifying an account is actually the customer.

² "Fighting Fraud with the Red Flags Rule: A How-To Guide for Business," Federal Trade Commission, March 2009. <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

³ "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft," *FTC Business Alert*, Federal Trade Commission, June 2008. <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtml>.

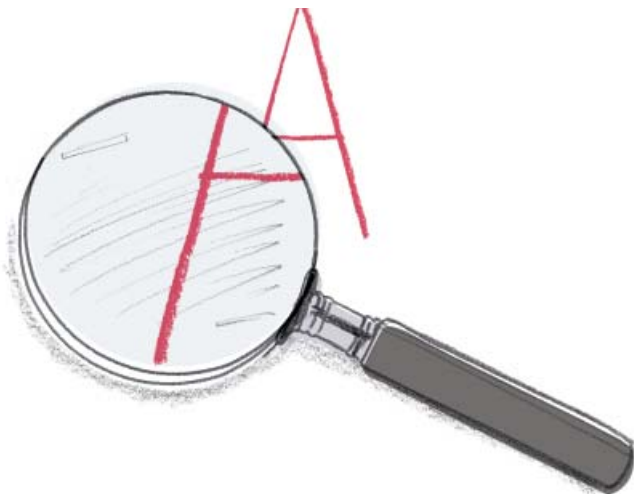
The Red Flags Rule: What financial institutions need to know

What does the rule require?

The Red Flags Rule requires that financial institutions and creditors implement a plan to identify, detect and respond to attempts to use stolen identity information. The FTC did not specify exactly what the indicators of potential identity theft might be. Instead, it requires your institution to take a risk-based view of operations and identify where and how a thief could be using someone else's identity to steal from your institution.

The rule envisions that institutions will identify potential identity theft through the use of red flags. The rule requires you to identify all of the indicators that might tip you off to possible identity theft, implement appropriate predictive and detective controls, and react appropriately according to the level of risk (e.g., if you suspect you have been given fake documents, do not open an account). Implement controls to verify items such as Social Security numbers, names and addresses.

Although the rule allows great leeway in determining which red flags are relevant to your institution, it is very specific about what you have to do and how you have to do it. The Red Flags compliance program must be adequately designed, documented and regularly updated. It must be approved and regularly reviewed by the board of directors. Sufficient training must be delivered. If you've outsourced pieces of your business operations where an identity thief might strike, you're required to ensure that your outsourcer has a thorough Red Flags plan in place.



Unique rule characteristics

Unlike many other federal regulations, the rule does not provide a rigorous checklist of specific red flags for which you must be on the lookout. Instead, it recognizes that identity theft techniques are changing faster than the agencies could possibly update the regulations. The rule lists 26 possible red flags that you may want to consider, but you're not required to use all (or even any) of these possible indicators in your program. The burden of determining how someone could steal from your institution is yours.

The rule also recognizes that your business may change over time, and those changes may affect the red flags you need to monitor. Mergers, acquisitions, alliances, joint ventures, outsourcing and in-sourcing events will likely trigger the need for a reassessment of your Red Flags plan. This is not a do-it-once-and-put-it-in-a-drawer regulation.

Note that the expansive scope of the rule means that compliance will touch many parts of your institution. CEOs, CFOs, COOs, chief legal officers, chief compliance officers, chief risk officers, information security officers and even your security department may need to be involved. It will impact your people (through training requirements), your processes (specifically those that govern how you react to a red flag event) and your technology (through automated controls and checks).

Finally, the FTC believes that Red Flags compliance is important enough to be dealt with at the board of directors' level. The board (or, lacking a board, a member of senior management) must approve the initial plan and review it on at least an annual basis. In addition, the plan must be administered by a senior resource, up to and including the audit committee.

The Red Flags Rule requires that financial institutions and creditors implement a plan to identify, detect and respond to attempts to use stolen identity information.

If your institution already has a Red Flags program in place, now is a good time to ensure its effectiveness.

Building a plan

If you do not already have a plan in place, the risk-based underpinning of the rule gives you considerable flexibility to formulate a plan that is effective without being overly burdensome. Protecting yourself against thieves is a good business practice, and your initial Red Flags Rule compliance plan may incorporate documenting and reinforcing many of your existing controls.

Your compliance strategy should begin with an assessment, and this assessment should be driven by two critical factors:

- the number of covered account types, and
- the number of ways those accounts are created and accessed.

The combination of these two factors will determine where you will need controls in place and how many of them you will need.

Once these two factors are quantified, there are a number of other things that you should consider:

- Have you been defrauded before by someone using stolen information? How was it done?
- What new techniques are identity thieves using?
- Do you already have some controls in place that can be incorporated into your Red Flags plan?
- What new controls are needed? Are they process- or technology-based?
- How many users will need to be trained?
- What reporting is appropriate for your situation?

Because the Red Flags Rule is new, there is no real case law to give you guidance as to how rigorous your plan should be. We believe it would be prudent to steer a middle course – don't go overboard, but don't create a simple checklist and hope for the best.

Assessing your existing plan

If your institution already has a Red Flags program in place, now is a good time to ensure its effectiveness. According to the FTC's guide, all institutions are required to have a written Identity Theft Prevention Program, which "must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones." In addition, the program must be appropriate to the size and complexity of your business and the nature and scope of its activities. Institutions that only have "check-the-box" plans will not be able to withstand regulatory scrutiny or deter identity theft. Start the risk assessment process by comparing the Red Flags Rule requirements with the controls in your existing plan. A gap analysis will help identify how to enhance current controls.

Is doing nothing an option?

Non-compliance is always an option – but it's not a good one.

The FTC has extended the deadline from Nov. 1, 2009, to June 1, 2010. After June 1, 2010, any occurrence of identity theft at your institution will expose you to an FTC investigation. We believe that enforcement of this rule will be complaint-driven, and given the staggering number of identity thefts, there will be no shortage of complaints.

Upon receipt of a complaint, the FTC may launch an investigation, review your institution's plan and determine whether it was reasonable. At this point, no one knows exactly what reasonable means, but it's a pretty good bet that a plan that has allowed multiple identity thefts will not rise to the reasonable level.

Given the financially devastating consequences of identity theft, you can also expect any enforcement actions to be well-publicized and the reputational damage to be significant. Explaining how a major theft happened and how it got past your institution's Red Flags plan is not something you want to discuss on the 6 o'clock news.

The Red Flags Rule: What financial institutions need to know

Initially, the FTC can assess penalties for violations retroactive to the June 1, 2010 enforcement date, require additional compliance reporting from you and obtain an injunctive compliance order. Further violations can result in a visit to federal district court and a fine of up to \$16,000 per occurrence of identity theft.

On the litigation side, there are two risks associated with non-compliance. First, state attorneys general may be able to file class-action suits under “unfair and deceptive acts and practices” theories. These actions usually permit both actual and punitive damages, and can include attorneys’ fees and court costs.

The greater litigation risk, however, will come from injured parties who file suit against financial institutions that did not prevent identity theft. The cost, effort and aggravation associated with repairing damaged credit and incorrect records can be significant, and in today’s litigious environment, injured parties will be looking for a target. If you are sued by one of these injured parties, expect that the plaintiff’s first request will be, “Please show me your Red Flags compliance program.” If you don’t have one, or it is poorly written and/or executed, the plaintiff will likely allege a breach of duty to protect the information.

In summary, the Red Flags Rule is likely to become the standard of care that all companies, not only financial institutions, will need to provide in order to prevent identity theft. Skipping Red Flags compliance will expose you to real regulatory, reputational and litigation risks. •

Do's

- Do** remember to update your plan when you have a significant change in your business.
- Do** get your board and internal controls team up to speed on compliance requirements.
- Do** use people with appropriate skills. Your plan will likely incorporate legal, security, fraud, technical and business process expertise.
- Do** perform an assessment before you build your program. There’s no need to put controls over accounts that aren’t covered.
- Do** talk to peers in your industry. Chances are many of your risks are similar.

Don'ts

- Don't** expect the Red Flags Rule to just go away. The public demand for identity theft protection is too great.
- Don't** put something together hastily. Your plan may have to withstand the scrutiny of an investigator.
- Don't** over-engineer your program. The bad guys are coming up with new ideas faster than you can update a too-detailed plan.
- Don't** forget to get Red Flags assurances from your outsourcers.
- Don't** underestimate training efforts. Keeping skilled identity thieves at bay requires people who know what to look for and what to do when they see it.
- Don't** ignore the rule. In today’s world, active denial of a federal regulation is a very bad idea.

Content in this publication is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information on the issues discussed, consult a Grant Thornton client service partner.

www.GrantThornton.com

© Grant Thornton LLP
All rights reserved
U.S. member firm of Grant Thornton International Ltd

The Red Flags Rule: What financial institutions need to know

How can Grant Thornton LLP help?

Understanding how to comply with this new, complex regulatory requirement, without creating unnecessary cost, complexity and burden, is not a simple task. Grant Thornton's Red Flags Compliance Services are designed to gather the information you need in order to determine your institution's compliance approach. Using our business-centric approach, we can help you answer the following questions:

- What types of identity fraud are you vulnerable to?
- What types of controls would you need to achieve compliance?
- What are the costs of compliance?
- What are the costs and risks associated with non-compliance?
- What are your solution alternatives?

Using a combination of automated surveys, structured interviews and reviews of already available documentation, we can deliver the necessary information to evaluate or help build your institution's Red Flags compliance program. Our professionals are well-versed in the operations of financial institutions, and our combination of business control, security, regulatory and technical experience ensures your Red Flags plan addresses security and identity theft issues in a methodical and efficient manner. We believe that compliance is a risk-based business decision that can only be made with good information.

For more information, contact one of our Red Flags Compliance Services professionals:



Forrest Frazier
Partner
Business Advisory Services
T 704.632.6801
E Forrest.Frazier@gt.com

Forrest is a partner in the Business Advisory Services practice of Grant Thornton's Charlotte office and has 15 years of experience in public accounting. He has experience with a wide variety of consulting, accounting and assurance engagements, including: financial and operational improvement; revenue enhancement and cost containment; controls and process design; consulting and remediation; Sarbanes-Oxley compliance; internal audit outsourcing, co-sourcing and transformation; enterprise risk assessments; non-financial surety engagements, including SAS 70 reviews; financial statement audits of public and private companies; forensic accounting and fraud investigations; due diligence related to buy and sell transitions; and project management.



Jan Hertzberg
Executive Director
Advisory Services
T 312.602.8312
E Jan.Hertzberg@gt.com

Jan leads the Chicago Business Advisory Services Information Technologies group. He has more than 20 years of experience helping multinational companies in banking, financial services, health care and telecommunications develop infrastructure, systems and internal IT controls for enhanced reliability and regulatory compliance. He currently serves as Grant Thornton's National Champion for Information Security/Privacy and leads the firm's initiative to enhance its security risk assessment methodology. Jan has held leadership positions with Fortune 100 companies, including IBM, Abbott and Ernst & Young LLP. As an IT audit and consulting practice leader, Jan has managed teams providing a range of services to the banking industry, including FFIEC-readiness reviews, internal vulnerability scans, external network penetration testing, social engineering and GLBA/privacy audits.



Jay Brietz
Senior Manager
Advisory Services
T 704.632.6916
E Jay.Brietz@gt.com

Jay is a senior manager in the Carolinas Advisory Services practice, and he is responsible for delivering solutions related to risk management, internal controls and process improvement opportunities. Jay helps lead the Carolinas SAS 70 practice and he serves on the national SAS 70 task force. Jay recently completed a three-year rotation in Grant Thornton's National Corporate Governance Group, where he was a contributing author to COSO's *Guidance on Monitoring Internal Control Systems*. Jay joined Grant Thornton in 2002 and is primarily aligned with the Financial Services industry group. He has more than 17 years of finance and accounting experience, including six years as an auditor in the Financial Services practice of a Big Four accounting firm, two years as an internal auditor for a global insurance company and two years as a financial consultant in the Finance and Performance Management practice of a large consulting firm.



Matt Thompson
Senior Manager
Business Advisory Services
T 336.271.3932
E Matthew.Thompson@gt.com

Matt is a senior manager in the Carolinas Advisory Services practice. He has more than 14 years experience working in the financial services industry. Since joining Grant Thornton LLP in 2002, Matt has worked with more than 30 financial institutions and has managed engagements that include co-sourced and outsourced internal audits, information security assessments, business continuity and disaster recovery preparedness engagements, Sarbanes-Oxley 404 assessments, information technology audits and more. Prior to joining Grant Thornton, Matt spent more than seven years in internal audit for a large financial institution, focusing on the internal audit, information technology and business process risk control arenas. In addition, he performed internal audit risk assessments for the bank's operations located throughout the United States, Hong Kong, Brazil and the United Kingdom.