

The Red Flags Rule: What not-for-profit organizations need to know

Grant Thornton LLP Advisory Services

The Red Flags Rule (FTC 16 CFR 681) compliance deadline is fast approaching, and many not-for-profit organizations are not prepared. This is largely because they 1) have never heard of the rule, 2) don't think they are covered by the rule or 3) have been distracted by other priorities. This paper will give you an overview of the rule, a view of several unique features of the rule, things to consider when formulating your compliance strategy, and a few do's and don'ts.



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 most recent statistics available regarding identity theft in the U.S. will show you why. In 2008 alone...

- the number of identity fraud victims rose by 22% to 9.9 million American adults
- 7.5% 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 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. That is what the Red Flags Rule attempts to do – close the loop on identity theft by making it harder for criminals to use stolen identities.

What does the rule require?

The Red Flags Rule requires that financial institutions and creditors (more on that later) implement a plan to identify, detect and respond to attempts to use stolen identity information. To its credit, the FTC did not specify exactly what the indicators of potential identity theft might be.

Instead, it requires your organization to take a risk-based view of your operations and identify where and how a thief could be using someone else's identity to steal from you.

The rule, however, was purposely written by the FTC to cover virtually any organization that does not require full payment up front. The rule defines a creditor as any business that allows a customer to defer payment. **In short, if you send invoices, you're probably covered by this rule.**

The rule envisions that organizations will identify potential identity theft through the use of red flags. A red flag might be a student presenting suspicious credentials, multiple address changes in a short period of time or a notification from a credit reporting agency that the student has placed a hold on his or her credit history. 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.

While the rule allows leeway on determining which red flags are relevant to your organization, it is very specific on 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. Adequate training must be delivered. If you've outsourced pieces of your organization operations where an identity thief might strike, you're required to ensure that your outsourcer has an adequate Red Flags plan in place.

In short, if you send invoices, you're probably covered by this rule.

Who must comply?

The Red Flags Rule does not name specific types of organizations that must comply. For higher education institutions, compliance requirements are based on the types of accounts your institution has with students.

The rule is generally based on the existence of covered accounts. The first type of covered account is one that is "a continuing relationship established by a person with... a creditor to obtain a product or service for personal, family, household, or business purposes." This definition may include many of the following:

- **clubs, associations, and other non-profit organizations that allow people to pay dues or pledges in installments**
- **hospitals and clinics that do not require full payment at discharge**
- **colleges, universities and schools that do not require full tuition payment at the time of enrollment**
- retailers that allow payment plans or issue private credit cards
- utilities that bill in arrears (for example, government and private water utilities that bill for actual water usage at the end of the month)
- professional service providers (law firms, accountants, doctors and dentists) that bill after service is delivered
- automotive dealers and affiliated loan institutions that arrange credit for buyers
- mortgage brokers, realtors and others in the real estate industry, and
- debt collectors, loan processors, and others who handle credit accounts.

The risk-based approach also carries into the second definition of a covered account. 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 you have prior history of identity thieves successfully using stolen information in your organization, that account will likely meet the "reasonably foreseeable" test. In addition, the FTC has stated that accounts with businesses (e.g., a sole proprietorship) may be covered by the rule – regulation is not limited to consumer-only accounts.

Remember, it's not the type of business you are, or the industry you're in — it's whether you have or handle covered accounts.

The Red Flags Rule: What not-for-profit organizations need to know

Unique rule characteristics

Unlike many other federal regulations, the rule does not provide a rigorous checklist of specific red flags that you must be on the lookout for. 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 you is yours.

The rule also recognizes that your organization 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 re-assessment 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 organization. CEOs, CFOs, COOs, chief legal officers, chief compliance officers, chief revenue 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 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 you is yours.

What's my compliance strategy?

Fortunately, the risk-based underpinning of the rule gives you considerable leeway to formulate a plan that is effective without being overly burdensome. Protecting yourself against thieves is good business practice, and your initial Red Flags Rule compliance plan may incorporate documenting and re-enforcing 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? Are there known identity theft techniques used against your industry? Do you already have some controls in place that can be incorporated into your Red Flags plan? How many 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?

Since the Red Flags Rule is new, there is no real case law to give you guidance of how rigorous your plan should be. We believe it would be prudent to steer a middle path – don't go overboard, but don't slap something together and hope for the best.



The Red Flags Rule: What not-for-profit organizations need to know

Is doing nothing an option?

Non-compliance is always an option – but it's not a very 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 business exposes 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 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. You can also expect any enforcement actions to be well-publicized, and the reputational damage to be significant.

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. The first is through state attorneys general, who 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 greatest litigation risk will come from injured parties who file suit against organizations that did not prevent identity theft. The cost, effort and aggravation associated with repairing damaged credit 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 will need to provide 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 environment, active denial is a very bad idea.

Contact information



Mark Oster
Principal-in-Charge
Business Advisory
Services
Not-for-Profit and Higher
Education Industry
Practice

T 212.542.9770
E Mark.Oster@gt.com

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