

The Red Flags Rule: What health care businesses need to know

Grant Thornton LLP Advisory Services

The Red Flags Rule (FTC 16 CFR 681) compliance deadline is fast approaching, and many hospitals and health care providers 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 provide you with an overview of the rule, a view of several unique features of the rule and how they relate to the health care industry, actions to consider when formulating your compliance strategy, and a few do's and don'ts.



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 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 a stolen identity.

Medical identity theft – a double dose of problems

The Red Flags Rule is especially relevant in the health care industry. The FTC estimated that more than 200,000 cases of medical identity theft occur each year, but because medical records are difficult to examine (due to HIPAA privacy restrictions), many experts believe the number is much higher.

Medical identity thieves are actively exploiting the gaps in identity theft prevention. To complicate the problem, in many cases the theft occurs inside the provider's organization and is extremely difficult to detect. Here are just some of the ways that identity thieves steal from you:

- **Obtaining illegal and fraudulent treatment.** Individuals with insurance billing system expertise have been caught billing a victim's health plan for fraudulent or overstated treatment claims. In other cases, an organized theft ring will use this technique. The ring will purchase stolen patient information on the black market and set up non-existent clinics to make fraudulent claims against the health policies of unknowing victims.
- **Buying addictive drugs.** Medical personnel with access to sensitive identity information may use that data to obtain prescription drugs either to sell or to satisfy their own addictions. Dishonest medical professionals have billed the insurance policies of identity theft victims for narcotics and have been known to call in prescriptions in a patient's name but pick it up themselves.
- **Obtaining free treatment.** Medical identity thieves may use stolen information to receive free medical treatment, courtesy of the identity theft victim. In this situation, thieves assume the identity of a victim by presenting a stolen insurance or Medicaid card at the time of treatment. This information is so valuable on the black market that there are known instances of identity thieves regularly canvassing poor neighborhoods and purchasing Medicare and Medicaid card numbers with fast food gift certificates.

While the financial consequences to the health care provider are significant, the impact on the identity theft victim can be devastating. Identity theft in the health care business is potentially deadly. Indeed, the World Privacy Forum has labeled medical identity theft as "the information crime that can kill you."

Victims of medical identity theft may have to deal with problems that range far beyond the financial. Here are just a few examples:

- **Ruined credit.** Medical identity thieves can easily run up massive bills that will never be paid – and the burden of cleaning up the personal credit damage falls to the victim. Clearing credit records that reflect these charges can take years, during which time the victim may be subjected to dunning calls, increased cost of borrowing or even the inability to get a job.
- **Loss of health coverage.** Once a medical identity thief (or ring of thieves) has obtained a valid insurance card number and associated personal information, they can easily run up enough charges to max out a policy. Usually, the first time the victim knows this has happened is when they receive a message from their insurance carrier informing them that they no longer have coverage. While the mess is being corrected, the victim may not be able to obtain treatment due to lack of coverage.
- **Inaccurate records.** Medical identity theft can threaten your patient's health – or even his/her life. If a medical identity thief successfully obtains treatment, their medical information can be co-mingled with that of the victim. In other cases, the thieves' information may be used to create an entirely new (and entirely wrong) medical record. This inaccurate information could be deadly – the bogus records may include inaccurate blood types, medication allergies and treatment histories. The false diagnoses now in the victim's records (for example, mental illnesses) may prevent the victim from obtaining coverage or working in a new job. Worse, the implementation of electronic medical records makes it extremely difficult to locate and correct all of the instances of an incorrect record.
- **Legal problems.** Medical identity theft can have serious legal implications to its victims. In Utah, a pregnant woman with a drug addiction stole the medical identity of an innocent mother and delivered a baby who tested positive for illegal drugs. Social workers subsequently contacted the actual owner of the identity and informed her they were coming to remove her children from the home. She had to hire a lawyer and undergo a DNA test to keep her family.

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 business 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 company 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 most likely covered by this rule.**

The rule envisions that businesses will identify potential identity theft through the use of red flags. A red flag might be a patient presenting suspicious credentials, multiple address changes in a short period of time or a notification from a credit reporting agency that the patient 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 great leeway on determining which red flags are relevant to your businesses, 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 business 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 businesses that must comply. Instead, compliance requirements are based on the types of accounts your business has.

The rule is generally based on the existence of covered accounts. A 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 net catches many of the following:

- hospitals and clinics that do not require full payment at discharge
- professional service providers (doctors, dentists, veterinarians, law firms and accountants) that bill after service is delivered
- retailers who 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)
- colleges, universities and schools that do not require full tuition payment at the time of enrollment
- automotive dealers and affiliated loan institutions that arrange credit for buyers
- clubs and non-profit organizations that allow people to pay dues or pledges in installments
- 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 a prior history of identity thieves successfully using stolen information in your business, that account will likely meet the "reasonably foreseeable" test. In addition, the FTC has stated that accounts with businesses (e.g., a pharmacy, clinic or physician's practice) may be covered by the rule – regulation is not limited to consumer-only accounts.

The Red Flags Rule: What health care businesses need to know

Health care providers have a special set of problems associated with the Red Flags Rule. Due to the large numbers of providers (pharmacists, specialty physicians, clinics) and payers (private insurance, Medicare, Medicaid, state-run programs), there may be hundreds of different account types that fall into the category of a covered account. Even those accounts that do not normally permit payment over time may be covered under the “reasonably foreseeable” language. Finally, as financial and medical information becomes more and more digitized, the number of places where fraud could occur is growing rapidly.

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.

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 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 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.

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? What new techniques are identity thieves using? 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 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.



Michael Di Paolo
Director
Grant Thornton LLP
Advisory Services

T 214.561.2520
E Michael.DiPaolo@gt.com

Michael Di Paolo is an advisory services director in Grant Thornton's Dallas office. With 25 years of experience in the information technology and consulting industries, Michael brings a wide variety of experience to the practice. Michael's broad range of experience includes IT strategy and planning, IT assessments, IT security, IT service management process alignment through ITIL®, IT governance, and Electronic Discovery pre-litigation assessments and solutions. He has significant experience in information management security, solution selections, ERP quality assurance, business process improvement, and application integration.

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

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 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.

Given the financially devastating – and potentially deadly – consequences of medical identity theft to its victim, 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 Red Flags plan is not something you want to discuss on the six o'clock news.

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 hospitals and other providers that did not prevent identity theft. The cost, effort and aggravation associated with repairing damaged credit and incorrect medical 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 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 world, active denial of a federal regulation is a very bad idea.