FTC Business Update

Federal Trade Commission ■ Bureau of Consumer Protection

The "Red Flags" Rule: What Telecom Companies Need to Know About Complying with New Requirements for Fighting Identity Theft

by Tiffany George and Pavneet Singh
Federal Trade Commission

As many as nine million Americans have their identities stolen each year. The crime takes many forms. Thieves may buy a car, obtain a credit card, or establish telephone or Internet service using someone else's identity. Consumers may not find out they're victims of identity theft until they review their credit reports or read their monthly statements and notice charges they didn't make – or until they get a call from a debt collector.

For millions of consumers, identity theft inflicts economic, psychological, and emotional harm. Victims may have to spend money and time repairing the damage to their good name and credit record. The cost to business can be staggering as well, with charges racked up by identity thieves unpaid and uncollectable.

Telecommunications companies may be the first to spot the red flags that signal the risk of identity theft, including suspicious activity suggesting that crooks may be using stolen information to establish service. That's why you need to know about a new law that requires many businesses – including most companies that provide telecommunications services to consumers – to spot the red flags that can be the telltale signs of identity theft and do something about them.

The new regulation – called the Red Flags Rule – requires companies to develop a written "red flags program" to detect, prevent, and minimize the damage that could result from identity theft. The Federal Trade Commission, the nation's consumer protection agency, enforces the Red Flags Rule.

The FTC will begin enforcing the Rule on May 1, 2009. Is your company required to comply with the Red Flags Rule? If so, what's your next step?

WHO MUST COMPLY

Companies that provide telecommunications services may be covered by provisions of the Rule that apply to "creditors." The Rule includes some specific definitions and exceptions, but it boils down to this: If your company regularly bills customers after services are provided, you are a creditor under the new law and will have to develop a written program to identify and address the red flags that could indicate identity theft in your covered accounts. The rule defines a "covered account" as a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft.

SPOTTING RED FLAGS

The Red Flags Rule gives telecom companies the flexibility to implement an identity theft prevention program that best suits their business, as long as it conforms to the Rule's requirements. The Rule requires that your program identify relevant red flags, detail your process for detecting them, describe how you will respond to them to prevent and mitigate identity theft, and spell out how you will keep your program current. Many companies already have fraud detection or prevention procedures they can incorporate into their program. Your program should be appropriate to the size of your organization, as well as to the nature of your business.

What red flags signal identity theft? There's no standard checklist, but here are a few signs that may arouse your suspicions:

- ***Alerts, notifications or warnings from a consumer reporting agency.*** For example, if a fraud alert is included with a credit report, federal law requires you to take reasonable steps to verify the identity of the customer who wants to open an account with you. If you find out that there's a credit freeze in place, you may want to follow up and ask for more information.

- ***Suspicious documents.*** Has an applicant given you identification documents that look altered or forged? Is the physical description on the identification inconsistent with what the applicant looks like? Is other information on the identification inconsistent with what the customer's told you? More investigation may be required.

- ***Suspicious personally identifying information.*** Personal information that doesn't match what you've learned from other sources may also be a red flag of identity theft. For example, if the current address doesn't match the address in the consumer report – or if the Social Security Number doesn't match the date of birth – fraud could be afoot. If the address on the application is fictitious or a mail drop – or if the only contact information is a pager – there may be a problem.

- ***Suspicious activity relating to a covered account.*** Did a customer ask for a new cell phone or add a new authorized user soon after a change of address? Did a customer's use patterns abruptly change? Did a new customer fail to make the first payment or make an initial payment but no others? Is mail returned repeatedly as undeliverable even though transactions still are being conducted on the account? Don't ignore the voice of experience when it tells you that something seems questionable.

- ***Notices from victims of identity theft, law enforcement authorities, or others suggesting that an account may have been opened fraudulently.*** Cooperation is key. Heed warnings from others that identity theft may be ongoing.

Of course, a red flag by itself may not indicate ID theft, but may be relevant in a larger context.

SETTING UP AND WRITING DOWN YOUR RED FLAGS PROGRAM

Once you've identified the red flags that are relevant to your business, your program should include the procedures you have put in place to detect them in your day-to-day operations. Your program also should describe how you plan to prevent and mitigate identity theft. How will you respond when you spot the red flags of identity theft? Will you close questionable accounts or monitor them more closely? Will you contact the consumer directly? When automated systems detect red flags, will you manually review the file? Finally, because identity theft threats change, consider how you will keep your program current to ensure you address new risks and trends.

No matter how good your program looks on paper, the true test is how it works. According to the Rule, the program must be approved by your Board of Directors or – if your company doesn't have a Board – by a senior employee. The Board may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff, and provide a way for you to monitor the work of your service providers. The key is to make sure that all members of your staff are familiar with the Rule and the new compliance procedures.

WHAT'S AT STAKE

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties. But even more important, compliance with the Red Flags Rule assures your customers that you are doing your part to fight identity theft.

For more information about designing a compliance program and your compliance responsibilities, email ***RedFlags@ftc.gov*** or visit ftc.gov.

Tiffany George and Pavneet Singh are attorneys in the Federal Trade Commission's Bureau of Consumer Protection.