

THIS MONTH'S TOPIC ...

News Tools to Combat Identity Theft Red Flag Guidelines Debut in May

In these trying financial times, everyone has a role to play in curbing the rising identity theft epidemic. As individuals, we can take steps to protect ourselves from becoming victims; however, it is government and business that can effect the most widespread change.

That's where the "Red Flag Rules" come in. Administered by the Federal Trade Commission and effective May 1, the guidelines provide credit-extending businesses with a baseline means of detecting identity-related fraud. This month, Identity Theft 911's Chief Privacy Officer Eduard Goodman and Betsy Broder, assistant director of the FTC's division of privacy and identity protection, explain [how the rules affect businesses](#) and [26 ways to mitigate risk](#).

["A Ray of Light as the Perfect Storm Persists?"](#) is a call for the private sector to abide by the regulations and ramp up overall anti-identity theft measures. A crime that knows no bounds calls for a collective response. We hope these new provisions help streamline it.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: media@identitytheft911.com

May 13, 2009

PLEASE NOTE

Since this newsletter was published, the Red Flag compliance deadline has been extended again, now to August 1, 2009.

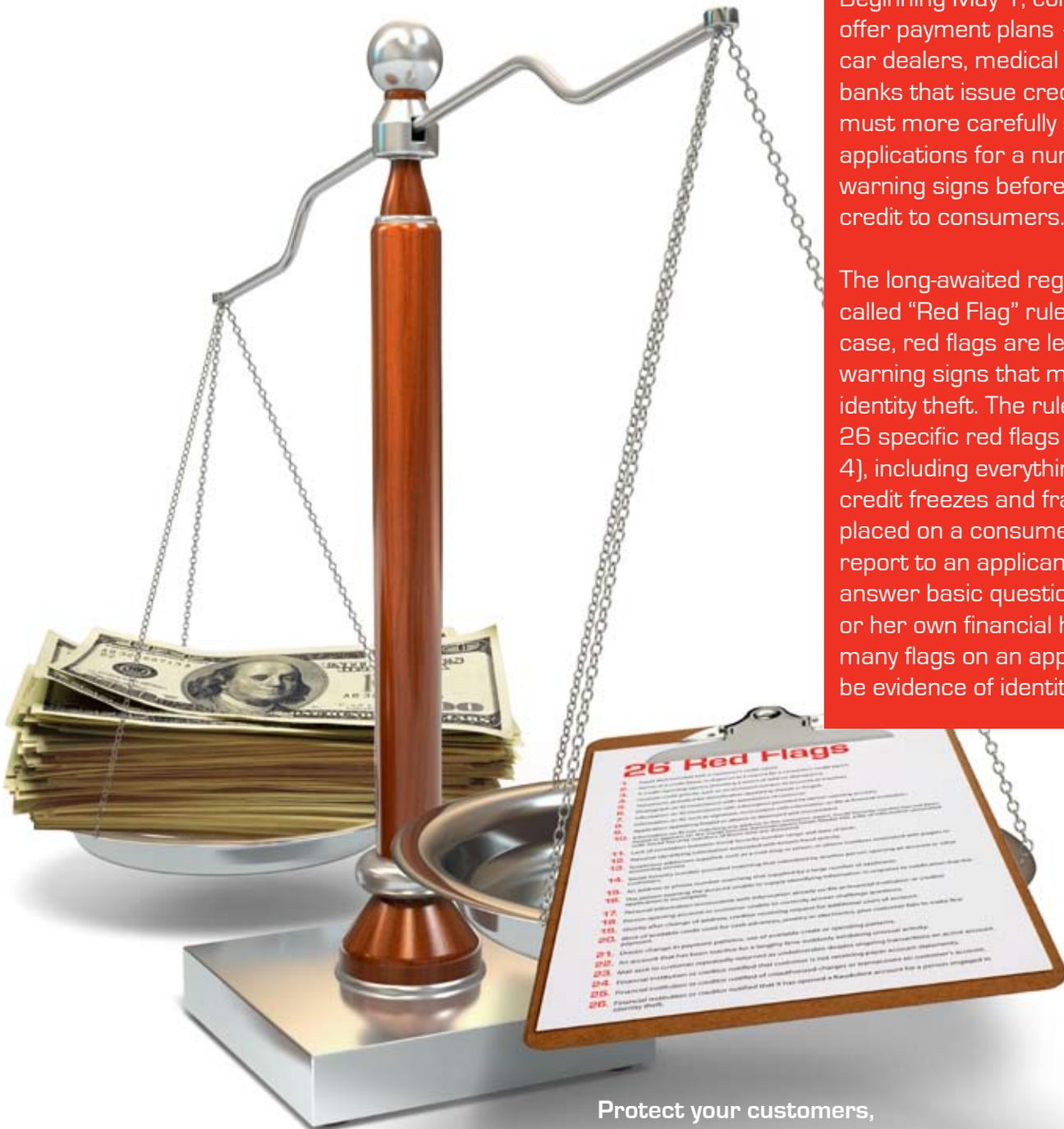


The Game of Identity Theft Hot Potato Ends on May 1

Businesses of all sizes must be ready to comply with **red flag** regulations... finally!

It's been a long time coming, but soon federal law will require more than 11 million businesses to be on perpetual high alert against identity theft. Beginning May 1, companies that offer payment plans – including car dealers, medical offices and banks that issue credit cards – must more carefully scrutinize applications for a number of warning signs before extending credit to consumers.

The long-awaited regulations are called “Red Flag” rules. In this case, red flags are legitimate warning signs that may indicate identity theft. The rules identify 26 specific red flags (see page 4), including everything from credit freezes and fraud alerts placed on a consumer’s credit report to an applicant failing to answer basic questions about his or her own financial history. Too many flags on an application may be evidence of identity theft.



Protect your customers,
or pay the penalties?

Therefore, companies must:

Identify which red flags may occur in their business

Detect red flags in real time, as credit applications are processed

Respond accordingly. Responses may include denying the credit application or alerting law enforcement, depending on the case.

Companies that choose to ignore the new rules may be investigated by the Federal Trade Commission (FTC) and fined civil damages for each violation.

Consumers have been waiting for these protections since 2003, when Congress passed the Fair and Accurate Credit Transactions Act (FACTA). The law mandated that federal bank regulators, the National Credit Union Administration, and the FTC establish procedures for identifying possible cases of identity theft. Originally, all businesses were supposed to have their red flag policies and procedures in place by Nov. 1, 2008, but only federally chartered banks and credit unions met the deadline. The FTC granted everyone else a six-month reprieve. The rules are now expected to take effect on May 1, 2009.

The message to businesses is clear.

"It's saying you have a duty, here and now, to stop identity theft," says Eduard Goodman, chief privacy officer at Identity Theft 911.

The Red Flag Regulations represent the federal government's first major attempt to work with the business community to mitigate the risk of identity-related fraud. The regulations are not meant to be a set of finite rules with direct and immediate consequences, but rather a baseline of knowledge from which businesses can make decisions. Just as physicians are trained to recognize the warning signs of disease, so too should businesses be aware of the warning signs of identity related fraud and use them to take adequate precautions.

"We are looking for good faith compliance—good faith efforts, particularly in the beginning when companies try to work through what their obligations are and get their programs approved," says Betsy Broder, assistant director of the FTC's division of privacy and identity protection.

The new enforcement regime is loosely defined by design, so as to encourage participation by the widest possible swath of credit-extending institutions. That's because some industries will never encounter certain red flags. The guidelines are comprehensive enough that every qualifying institution can use them to create its own protocols, Goodman says.

"Our initial step is to coax compliance and, as with many of our other law enforcement initiatives, when we do begin bringing cases, it most likely will be against entities that have high risk that have not taken even the most basic steps to implement the program," Broder says.

Small business owners may see the

Red Flag Regulations as a great deal of hullabaloo – and expense – over a simple credit application. But the rules were not drafted merely to protect consumers. They were intended to help businesses, as well. "We tell companies, this is about developing an anti-fraud program that should protect your bottom line," explains Broder. "It forces you to think more conceptually about having this single program— putting it in writing gives you that opportunity."

Who is affected?

As the calendar approaches May 1, the biggest question in the business community is: Who, exactly, must abide by the Red Flag Rules?

"The first step is to determine whether they are a creditor—that is, if they defer payment for a good or a service on a regular basis," Broder explains.

Next, companies must determine whether they offer "covered accounts." As defined by the FTC, these are accounts used primarily for personal, family or household purposes that permit multiple payments or transactions. The definition also includes any account that could be pose financial risk to the consumer, creditor or financial institution if corrupted by identity theft.

Businesses should not expect a knock on the door from the FTC telling them whether they must comply with the Red Flag Rules (with more than 11 million businesses estimated to fall under the regulatory umbrella, that would involve a lot of knocking). Instead,

“We don’t want this to become just another piece of bureaucratic paperwork that people create and file away,” Broder says.

responsibility lies with businesses themselves to conduct their own internal policy examinations. In FACTA, Congress was intentionally broad in its definitions of covered accounts in order to catch all the different ways an identity thief might try to get goods or services without paying for them.

Monthly veterinary bill payments, online music accounts, satellite radio subscriptions—the possibilities are manifold. “You don’t need to be a bank,” Goodman says of qualifying institutions. “You don’t need to offer a credit card.”

While a number of companies offer services intended to help businesses with red flag compliance, the good news for small businesses is that compliance doesn’t necessarily require hiring an outside contractor or an attorney.

“It’s not a zero-tolerance policy saying ‘you must prevent identity theft,’” says Goodman. “You just have to have a plan to try to prevent it.” For some businesses, the plan could involve creating a new,

automated system that screens credit applications, or upgrading an existing one. Other companies may use a series of manual checks and balances. Either the way, the process is the same: Scan for red flags. When you find one, investigate more closely. If information on an ID doesn’t match other documents filed by the applicant, for example, that may be time to pause the process and request a full credit report, Goodman says.

Businesses that are unsure whether the rules apply to them should err on the side of caution, Broder and Goodman say, and implement written policies and procedures intended to detect and address red flags. This could help them prevent fraud.

A question of enforcement

Because the Red Flag Regulations are rather loosely defined, it’s difficult to predict exactly how they will be enforced. For example, it’s not explicitly against the law to extend credit to an applicant whose circumstances elicit a “red flag.” Nor is it illegal to offer credit to someone whose application triggers two or three red flags. Instead, possible violations of the new rules will be investigated reactively, in the wake of identity fraud involving a particular business’ line of credit. Businesses that have some process in place to identify, detect and respond to red flags will likely satisfy the FTC’s requirements. Businesses that ignore Red Flag Regulations altogether could face civil penalties.

Broder is reluctant to discuss the agency’s enforcement strategy in

detail. But she said the FTC will be looking at its Consumer Sentinel database, where consumers file identity theft complaints, as a starting point. “One example would be if we see that a remarkably high number of accounts were opened at a particular creditor or financial institution fraudulently—that might signal that maybe they don’t have good fraud detection programs in place,” Broder says. “We sometimes do an assessment of a particular industry if we know that it is high risk. We’ll send out letters to an entity in that area and say ‘please provide us with information on how you have created and implemented your red flags program.’” She declined to mention which industries present high risks for identity theft-related fraud.

Broder stresses, however, that initial efforts are to encourage voluntary compliance. The FTC will make efforts to educate, and “to talk with people, to make sure that people understand what the rule is about and are taking the appropriate initial steps to get their programs in place,” she says.

After that, Red Flag Regulations require businesses to periodically reassess and update their red flag programs. This is an important part of the process, since “risk changes the way the bad guys operate,” says Broder.

“We don’t want this to become just another piece of bureaucratic paperwork that people create and file away,” Broder says. “I think when people get down to the brass tacks, it really is thinking about what you already do in your anti-fraud and fraud-protection programs and making it comprehensive.” ■

- 
- 1.** Fraud alert included with a consumer's credit report.
 - 2.** Notice of a credit freeze in response to a request for a consumer's credit report.
 - 3.** A credit-reporting agency providing a notice of address discrepancy.
 - 4.** Unusual credit activity, such as an increased number of accounts or inquiries.
 - 5.** Documents provided for identification appearing altered or forged.
 - 6.** Photograph on ID inconsistent with appearance of customer.
 - 7.** Information on ID inconsistent with information provided by person opening account.
 - 8.** Information on ID, such as signature, inconsistent with information on file at financial institution.
 - 9.** Application appearing forged or altered or destroyed and reassembled.
 - 10.** Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased.
 - 11.** Lack of correlation between Social Security number range and date of birth.
 - 12.** Personal identifying information associated with known fraud activity.
 - 13.** Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.
 - 14.** Social Security number provided matching that submitted by another person opening an account or other customers.
 - 15.** An address or phone number matching that supplied by a large number of applicants.
 - 16.** The person opening the account unable to supply identifying information in response to notification that the application is incomplete.
 - 17.** Personal information inconsistent with information already on file at financial institution or creditor.
 - 18.** Person opening account or customer unable to correctly answer challenge questions.
 - 19.** Shortly after change of address, creditor receiving request for additional users of account.
 - 20.** Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.
 - 21.** Drastic change in payment patterns, use of available credit or spending patterns.
 - 22.** An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.
 - 23.** Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.
 - 24.** Financial institution or creditor notified that customer is not receiving paper account statements.
 - 25.** Financial institution or creditor notified of unauthorized charges or transactions on customer's account.
 - 26.** Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft.

A Ray of Light as the Perfect Storm Persists?

EDITORIAL

Red Flag Guidelines Aim to Restrain the Rage

By Adam Levin



As the economy continues on its harrowing descent, the number of consumers whose finances are in dire straits grows exponentially. Many are finding that one more setback could pitch them into a financial void if they aren't already there. And while there are numerous factors that can throw any of us into the proverbial volcano, there is one that must and can be properly mitigated: identity theft.

In times of scarcity, everyone is desperate to maintain or to hold onto some semblance of their financial standing, this goes without saying. In that respect, however, identity thieves are no different from the rest of us. Recent identity theft statistics show that as legitimate revenue streams began to dry up last year, identity theft surged. That's The Perfect Storm in action. Keep in mind, too, that we're only talking about last year's numbers, as the storm gained momentum. Whether this storm has yet reached full force remains to be seen, but the statistics reflecting the

identity crimes committed this year likely won't be pretty.

To make the situation all the more unjust, we consumers can do everything within our own power to shore up our personal identifying information, but it doesn't count for everything. We can lock down, shred, encrypt, firewall, hermetically seal and redact to no end the information we have in our possession. We can have perfect data security protocol within our own homes, but if our data exists in a repository anywhere outside our home (and for most of us, it does), we still run the risk of a bank or business issuing credit to a criminal in our name. This has been the missing link in the chain of responsibility, and it has gone on for far too long.

Consumers aren't the only victims

Rarely does identity-related fraud claim a single victim. Consider the most common scenario: Identity thief

acquires Jane Doe's name, address and Social Security number; identity thief opens fraudulent credit cards in Jane Doe's name; identity thief uses cards to finance a \$15,000 shopping spree. In everyday cases like this one, who takes the hit? Obviously, Jane Doe—she's the one who must cancel the fraudulently acquired credit cards, straighten out bogus charges and deal with the damage done to her credit history.

But there are less obvious victims. Banks often swallow losses due to fraudulent credit card use. And if the perpetrator's crime spree included the use of a credit account opened with the local retailer, that retailer is also on the hook for that account's fraudulent purchases. Unfortunately, retail losses are often passed off to consumers by way of higher prices. A seasoned identity thief leaves behind a trail of scorched financial earth that everyone ultimately inhabits. The all-too-obvious conclusion: We all have a role to play in fixing this situation.

Enter the Red Flag Rules

Effective May 1, the Red Flag guidelines provide a structure for businesses to set up a systematic fraud prevention process. In their attempt to accommodate the needs of myriad credit-granting institutions, the Federal Trade Commission, banks and credit unions had to agree to settle on enforcement standards that are, by necessity, ambiguous. Extending credit in defiance of one, two or even five provisions is not grounds for an FTC action. Not having a plan that takes the Red Flag Rules into consideration is. Businesses are being asked only to consider best practices and make a good faith effort to incorporate them into their day-to-day operations. Once they know what needs to be done, it's up to the FTC to help ensure that it is. Sounds fair enough.

Compliance with the Red Flag Rules shouldn't be a problem for larger and mid-sized banks and financial institutions. Reporting either to the FDIC (banks) or the NCUA (credit unions), these lenders are already accustomed to having their lending practices under a regulatory microscope, and most have had programs that reflect the "Red Flag Rules" principles in place of years. But these businesses, by virtue of their size, have something that smaller businesses do not—that is, the resources to automate their lending policies and create enterprise-wide adjustments when the need be.

There may be more of a learning curve for smaller organizations that have less fiscal resources. That said, Red Flag Rules shouldn't be prohibitive or even difficult to incorporate. After all, many are common sense guidelines; businesses will likely find they're already abiding by them formally or informally. It's the cementing of policies in writing that concerns the government, as well as the question of whether businesses



are making a good faith effort to follow them.

A stitch in time...

Businesses shouldn't stop at the Red Flag Rules, however. Data breaches can be a potentially costly proposition, to say the absolute least. Any of the recent class action lawsuits filed against businesses responsible for data breaches can attest to this. Just look at the Starbucks Corporation, which became the object of a suit filed in a Seattle federal court this past February over a lost laptop that contained the names, addresses and Social Security numbers of 97,000 employees.

This is precisely why the Red Flag Rules should be made a part of a larger anti-fraud strategy that includes consideration for the issue of consumer data security. Businesses that aren't

already doing so should couple Red Flag strategies with policies designed to ensure the safe storage of sensitive medical, financial or personal identifying information in their possession.

The Red Flag Guidelines aren't a cure-all, though they may very well put us on the road to the paradigm shift that's been so desperately needed, in this age when our personal information (and thus, our financial well-being) is in the hands of many. While consumers must not fail to be vigilant in ensuring the safety of their own information, the time is long past due for businesses to have a better system to identify, detect and respond to identity theft among their customer base. There is no doubt, we each must be the guardians of our identities, but it's time credit-issuers did the same to the best of their ability. Trust us on this one: what's best for the consumer will ultimately be best for business. ■

26 Red Flags

1. Fraud alert included with a consumer's credit report.
2. Notice of a credit freeze in response to a request for a consumer's credit report.
3. A credit-reporting agency providing a notice of address discrepancy.
4. Unusual credit activity, such as an increased number of accounts or inquiries.
5. Documents provided for identification appearing altered or forged.
6. Photograph on ID inconsistent with appearance of customer.
7. Information on ID inconsistent with information provided by person opening account.
8. Information on ID, such as signature, inconsistent with information on file at financial institution.
9. Application appearing forged or altered or destroyed and reassembled.
10. Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased.
11. Lack of correlation between Social Security number range and date of birth.
12. Personal identifying information associated with known fraud activity.
13. Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.
14. Social Security number provided matching that submitted by another person opening an account or other customers.
15. An address or phone number matching that supplied by a large number of applicants.
16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete.
17. Personal information inconsistent with information already on file at financial institution or creditor
18. Person opening account or customer unable to correctly answer challenge questions.
19. Shortly after change of address, creditor receiving request for additional users of account.
20. Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.
21. Drastic change in payment patterns, use of available credit or spending patterns.
22. An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.
23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.
24. Financial institution or creditor notified that customer is not receiving paper account statements.
25. Financial institution or creditor notified of unauthorized charges or transactions on customer's account.
26. Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft.