

Now effective January 1, 2011, certain businesses in the United States are required to implement a written Identity Theft Prevention Program to detect warning signs (so called Red Flags) and to implement processes to quickly mitigate the impact of Identity Theft and to stop further instances.

On December 8, 2010, the Red Flag Program Clarification Act of 2010 passed in The House of Representatives. The Clarification Act limits the definition of a “creditor” under the Fair Credit Reporting Act to only those entities that use consumer reports, furnish information to consumer reporting agencies, or advance funds to or on behalf of a person. By using this definition, The Act now excludes law firms, health care practices, retailers, utility companies, telecommunications firms, automobile dealerships, and other small businesses from complying with the Red Flags Rule. The purpose of the revision is to ensure that the Red Flags Rule covers creditors who pose the highest risk for identity theft. The clarification is significant for health care entities, lawyers, accountants, other professionals, and small businesses that will not be subject to FTC regulation for any violation of the Red Flags Rule.

Question: What businesses must comply with the FTC Red Flag Rule?

The Red Flag Rule applies to businesses deemed to be either “financial institutions” or “creditors” and that have “covered accounts.” Of note is the FTC’s broad definition of “creditor” entities and “covered accounts.” These terms are broadly defined to include many types of businesses, across many industry classes.

“Creditor” – was originally defined in the Act to include any organization that “regularly defer payment for goods or services or provides goods or services and bills customers later,” including but not limited to lawyers, accountants, healthcare providers and telecommunication companies, etc. (See 15 U.S.C. Â§ 1681a(r)(5); 15 U.S.C. Â§ 1691a(d); 15 U.S.C. Â§ 1691a(e).) The definition also applied to those entities that provide loans or extend credit such as finance companies, mortgage brokers, retailers and car dealerships. The definition went one step further to include any entity that regularly engaged in the decision to extend, renew or continue credit, such as a third-party debt collector. The Clarification Act limits the definition of “creditor” to a person who obtains or uses consumer reports in connection with a credit transaction, furnishes information to consumer reporting agencies in connection with credit transactions, or advances funds based on the recipients’ obligation to repay.

“Covered Account” – this term is lynch-pin to whether an entity is required to comply with the Red Flag Rule. Any “financial institution” or “creditor” with either: 1) consumer accounts that permit multiple payments or transactions, or very importantly, 2) has any other account that presents a reasonably foreseeable risk of identity theft must implement a written Identity Theft Prevention Program.

Question: Does the FTC require the implementation of a specified type of ID Theft Program?

The FTC provides complete latitude on the type of program to be instituted since each organization has to manage its own unique set of exposures. The FTC does, however, require that any such program include four basic elements as follows:

Step 1: The Identification and compilation of a list of Red Flags specific to your Business – Red Flags are suspicious patterns, practices or activities that indicate that ID theft may be occurring. For example, the request to add a new card holder shortly after a change in a client’s mailing address may be a Red Flag.

Step 2: The detection of ID theft – Once potential Red Flags have been identified a set of processes must be implemented that will detect any such Red Flags. For example, if you have identified requests for new card holders shortly after an address change, you must establish a system notice to inform you when this occurs. This step will likely include employee education.

Step 3: Prevention and Mitigation of ID Theft – action protocols must be instituted that dictate what procedures will be taken to verify if an ID Theft event has/is occurring and what steps are to be taken to prevent or reduce the damage caused.

Step 4: Program Reevaluation – Since ID theft is an ever changing threat, the FTC requires that you repeat the above three steps periodically to ensure that your program anticipates new threats.

▶ To learn more about how AmWINS can help your clients who may be impacted by the FTC Red Flag Rule, reach out to your AmWINS contact or email marketing@amwins.com.



▶ AmWINS Group, Inc. is a leading wholesale distributor of specialty insurance products and services. AmWINS has expertise across a diversified mix of property, casualty and group benefits products. AmWINS also offers value-added services to support some of these products, including product development, underwriting, premium and claims administration and actuarial services. With over 1,800 employees located in 16 countries, AmWINS handles over \$5 billion in premium annually through our four divisions: Brokerage, Underwriting, Group Benefits and International.

Please note that the FTC requires that your board of directors, management committee or senior-level employee if no such board exists, formally approve the written program and appoint those responsible for implementing and administering the program.

Question: What are my liabilities for not complying with the Red Flag Rule?

There is no private right of action under the Red Flag Rule. Consumers can file a complaint with the FTC, but only a governmental agency can enforce the Rule. (See 15 U.S.C. Â§ 1681m(h)(8).) The FTC can seek monetary civil penalties as well as injunctive relief. The U.S. Department of Justice typically files such suits in federal court. The maximum penalty is \$3,500 per violation.

Question: Do we have to have to design and implement a Red Flag ID Theft Prevention Program if we already comply with data security requirements such as the Health Insurance Portability & Accountability Act (HIPAA) or the Financial Services Modernization Act of 1999?

The Red Flag Rule is not a data security regulation but rather a complement to data security procedures. Collecting only the personal information absolutely required for your business and providing notification to clients where a breach may have occurred are an integral part of your business requirements but handled separately from a legal standpoint.

Forty-six states have enacted security breach notification legislation. Requirements extend beyond notification in some states. Massachusetts, for example, effective March 1, 2010, requires encryption of confidential data when it is on a mobile device. Effective January 1, 2010, a similar law was enacted for any entity doing business in Nevada. We recommend that you speak to legal counsel about requirements in your state. Please do note, however, that you must adhere to each state's data protection and notification laws in which you collect personal information. The state requirements are triggered by breaches involving residents of that state, not where the offender is domiciled or the breach took place.

Question: Is there a way I can protect myself from exposure from claims brought directly by my clients/consumers or by a governmental agency?

Many insurers have developed what can be termed as "Cyber Liability" products. These products are designed to provide coverage for both first party and third party exposures to loss. The following summarizes some of the exposures that are insurable under a Cyber Liability policy.

FIRST PARTY	THIRD PARTY
<ul style="list-style-type: none"> • Loss of Private Data <ul style="list-style-type: none"> o Notification Costs o Forensic Costs o Crisis Management Expenses o Credit and Identity Repair Services • Business Continuity Expenses <ul style="list-style-type: none"> o Extra Expenses to Continue Operations o Business Income Loss o Restoration of Lost or Damaged Data • Cyber Extortion <ul style="list-style-type: none"> o Ransom Payments o Other Expenses 	<ul style="list-style-type: none"> • Client Suits – Privacy <ul style="list-style-type: none"> o Suits from clients alleging negligence in protecting information and other causes of action such as reputational injury • Client Suits – Denial of Service <ul style="list-style-type: none"> o Suits from clients alleging negligence in protecting the network against denial of service • Regulatory Liability <ul style="list-style-type: none"> o Regulatory fines and penalties where insurable o Consumer redress/restitution funds

For more information on the Red Flag Rule or Cyber Liability products please contact your insurance agent.

RESOURCES

1. The Red Flags Rule: ftc.gov/os/fedreg/2007/november/071109redflags.pdf
2. The FTC's Identity Theft Site: <http://www.ftc.gov/bcp/edu/microsites/idtheft>
3. Protecting Personal Information – A Guide for Business: <http://www.ftc.gov/infosecurity/>
4. Information Security Interactive Video Tutorial: <http://ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html>
5. Do-It-Yourself Template for Businesses at Low Risk for Identity Theft: <http://www.ftc.gov/bcp/edu/microsites/redflagrule/diy-template.shtml>
6. OnGuard Online Identity Theft Site Managed by the FTC: <http://www.onguardonline.gov/topics/identity-theft.aspx>