

## **Tax Practitioners Beware: New FTC “Red Flag” Regulations Will Probably Affect You**

Most CPAs, EAs and Tax Preparers will be affected by the new “Red Flag” regulations that will start to be enforced on November 1, 2009. These are the same regulations that apply to financial institutions not regulated by the FTC beginning last November.

The Federal Trade Commission (FTC) regulations, referred to as the “Red Flag Rules,” require financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACTA) Act of 2003.<sup>1</sup> (FTC Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.2)<sup>2</sup>

The regulations are referred to as “Red Flag Rules” because they require programs to be placed in operation by those affected businesses that will identify, detect, and respond to business practices or specific activities (referred to as “Red Flags”) that could result in identity theft. The programs must include procedures to protect against potential identity theft and provide a remedial procedure should identity theft occur.

We are providing a Free Word Document Template to help you develop your own policy and written rules. The template can be customized to your firm, but acts as the starting point in developing your Red Flag policy.

### **So what does this have to do with CPAs, EAs and Tax Preparers?**

The rules are applicable to “financial institutions” and “creditors” with “covered accounts.” CPAs, EAs and Tax Preparers certainly do not fall under the definition of a “financial institution.” However, depending upon how the business is operated, the CPA, EA or Tax Preparer may fall under the definition of a “creditor” with “covered accounts.” To fully understand the scope of these regulations as they may apply to CPAs, EAs and Tax Preparers, one needs only to understand the FTC’s definitions for “creditors” and “covered accounts.”

### **How can a CPA, EA or Tax Preparer be considered a creditor?**

Under FACTA, “creditor”<sup>3</sup> is defined the same way as in the Equal Credit Opportunity Act (“ECOA”), as:

- A. Any entity that regularly extends, renews, or continues credit;
- B. Any entity that regularly arranges for the extension, renewal, or continuation of credit; or
- C. Any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

The ECOA definition of “credit” includes a right granted to defer payment for any purchase. Thus, any person that provides a product or service for which the consumer pays after delivery is a creditor.

Thus, CPAs, EAs and Tax Preparers who do not collect their fee for services at the time the service is rendered and allows the client to pay for the service after completion of the service or delivery of the final product (for example, the finished tax return) is by definition a “creditor.”

Note, however, that according to the FTC’s “How-to-Guide for Business”<sup>4</sup> accepting credit cards as a form of payment does not in and of itself make an entity a creditor. But if a company offers its own credit card, arranges credit for its customers, or extends credit by selling customers goods or services now and billing them later, it is considered a “creditor” under the law.

### **What are covered accounts?**

Once it has been determined that a business or organization is a creditor, it must be determined if that business or organization has any “covered accounts,” as the Red Flags Rule defines that term. To make that determination, look at both existing accounts and new ones. Two categories of accounts are covered.<sup>5</sup>

- **Consumer accounts** – These are accounts that a business or organization offers to its customers that are primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.<sup>6</sup>
- **Any other kind of account** – A second kind of “covered account” is “any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to permit multiple payments or transactions – they always are “covered accounts” under the Rule – other types of accounts are “covered accounts” only if the risk of identity theft is reasonably foreseeable.

If a CPA, EA and Tax Preparer business qualifies as a “creditor,” the accounts receivable file (in whatever manner maintained) becomes a consumer account by the above definition.

### **Conclusion**

Since generally every CPA, EA and Tax Preparer, except for those that require all payments for services up front, will fall under the jurisdiction of the “Red Flag Rules,” steps should be taken by these businesses to comply with those regulations.

### **Consequences of non-compliance**

In the past, the FTC has been aggressive in the enforcement of consumer privacy rules, and the violation of the rules can result in civil penalties of up to \$2,500 per violation. But a much larger penalty could come as a result of the civil action brought by a client and an astute plaintiff attorney armed with the fact that the defendant did not abide by the “Red Flag Rules.” CPAs, EAs and Tax Preparers files and tax return data contain very sensitive client identity information. Think about it; a client file at the very least includes the name, address, SSN, W-2 information and probably a phone number and e-mail address, not to mention the bank routing number for the automatic deposit of a refund. Then, if a firm’s business practice is to scan and retain other documents, such as brokerage account statements, bank statements, 1099s, etc., the list of sensitive information begins to grow.

### **What are Red Flags?**

Applicable sections of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the Red Flags Rule, define a red flag as a pattern, practice or specific activity that indicates the possible existence of identity theft. The regulations provide guidance by listing five specific categories of red flags:

1. Alerts, notifications or other warnings received from consumer reporting agencies or service providers such as fraud detection services.
2. The presentation of suspicious documents.
3. The presentation of suspicious personal identifying information, such as a suspicious address change.
4. The unusual use of, or other suspicious activity related to, a covered account.
5. Notice from customers, victims of identity theft or law enforcement authorities.

Each organization is responsible for coming up with its own list of Red Flags, and the list should be as exhaustive as possible. Unfortunately, there is no specific set of red flags for every business. Even though a business belongs to the same industry as another, it may have different Red Flags because of the manner in which the business is operated. Each business must include every situation that can be envisioned.

### **Where do you go from here?**

If your CPA, EA or Tax Preparer firm qualifies as a “creditor” with “covered accounts” under the Red Flags Rule, as most will, you are required to take proactive measures to detect and prevent identity theft involving client data.

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs. Your Program must include four basic elements, which together create a framework to address the threat of identity theft. Each firm is required to implement a four-pronged identity theft prevention program as follows:

- **Step #1 – Identify Potential Red Flags** – A company’s program must include reasonable policies and procedures to identify the “red flags” of identity theft that might occur in the day-to-day operation of the business. Red flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account with the company, an ID that looks like it might be fake would be a “red flag” for the business.
- **Step #2 – Develop Detection Policies & Procedures** – You must develop policies and procedures to detect red flags. The program must be designed to detect the red flags that were identified in step #1. For example, if you have identified a fake ID as a red flag, you must have procedures in place to detect possible fake, forged, or altered identification.
- **Step #3 – Red Flag Responses** – The Program must spell out appropriate actions to be taken when red flags are detected in order to prevent and mitigate identity theft, such as contacting the customer, calling law enforcement, or some other appropriate action.
- **Step #4 – Periodically Update the Program** – A company must update their identity theft program periodically to handle any changes in risks to customers from identity theft. If the business is incorporated, the Board of Directors (or Board Committee) must approve the initial written program. A program must indicate who is responsible for administering the program and provide for staff training, if there is staff, and address how the company will insure its contractors’ compliance.

The Red Flags Rule gives a company the flexibility to design a program appropriate for the company – its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive program that addresses a high risk of identity theft in a complex organization, others with a low risk of identity theft can have a more streamlined program.

### “Starter Policy & Procedure”

To help CPAs, EAs and Tax Preparers develop their own compliance program, we have prepared a basic policy and procedure guide that can be customized to suit the way your firm conducts its business. Although, this starter policy and procedure may suit some smaller firms, it is not a “fit all” compliance program. Every business has its own unique mode of operation, and the program must be customized to fit each particular firm. In addition, using the starter policy and procedure is at your own risk; see the disclaimer at the end of the article.

### What about Service Providers?

Whenever a service provider is performing an activity for the firm in connection with a covered account, it is the firm’s responsibility to make sure that the provider (a) has an Identity Theft Prevention Plan, and (b) is following the Identity Theft Prevention Plan. The same requirement to detect, prevent and mitigate identity theft as it pertains to covered accounts is extended to any service provider who is engaged to perform an activity in connection with the covered accounts.

### Assisting your business clients

Now that you have thought about your own compliance issues, make your business clients aware of the Red Flag Rules and see if it will apply to their business. The regulations apply to any business who meets the criteria of a creditor and have covered accounts. That would include a dentist, chiropractor, financial planner, attorney, handyman, plumber and the list goes on. You might study up on the requirements and add Red Flag counseling as one of your services.

### **Coordination with other privacy and security rules**

In addition to the Red Flag Rules that apply to most CPAs, Eas and Tax Preparers, there are other privacy-related laws, regulations and rules that may apply to your firm:

- The **Gramm-Leach-Bliley Financial Modernization Act of 1999** (GLB Act) resulted in the issuance of the Privacy and Safeguards Rules by the FTC, which apply to traditional financial institutions as well as non-bank mortgage lenders, loan brokers, investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. While CPAs were provided with an exemption to the Privacy Rule in 2006, the Safeguards Rule remains applicable to Tax Preparers (including Enrolled Agents).
- For CPAs, **Rule 301 of the AICPA Code of Professional Conduct** and State Board of Accountancy Rules also apply to the handling of confidential client information.
- **IRC Sec 7216** and subsequent regulations requires all tax preparers to obtain consents from their clients to use or disclose tax return information.
- Individual states also have initiated their own laws with respect to privacy and security applicable to businesses.

<sup>1</sup> *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003: Final Rule. Federal Register / Vol. 72, No. 217 / Friday, November 9, 2007 / Rules and Regulations*

<sup>2</sup> *On November 9, 2007, the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration, published a joint notice of final rulemaking in the Federal Register (72 FR 63718) finalizing the Identity Theft Red Flags regulations and guidelines. This rule, promulgated pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), requires financial institutions and creditors to develop and implement written "identity theft prevention programs." The programs must provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft. Although the final rule became effective on January 1, 2008, full compliance with the rule is not required until November 1, 2008.*

<sup>3</sup> *Under FACTA, "creditor" is defined the same way as in the Equal Credit Opportunity Act ("ECOA"), as any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. The ECOA definition of "credit" includes a right granted to defer payment for any purchase. Thus, any person that provides a product or service for which the consumer pays after delivery is a creditor. The term "person" means "a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association." 15 U.S.C. § 1691a(f). See also Regulation B, 68 Fed. Reg. 13161 (Mar. 18, 2003).*

<sup>4</sup> *FTC How-to-Guide: <http://www2.ftc.gov/bcp/edu/microsites/redflagrule/index.shtml>*

<sup>5</sup> *An "account" is a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. 16 C.F.R. § 681.2(b)(1).*

<sup>6</sup> *See 16 C.F.R. § 681.2(b)(3)(i).*

## **Disclaimer**

*This information, the "Starter Policy & Procedure" and other suggestions presented in this material were developed from FTC documents and regulation analysis and are believed to be reliable but should not be construed as legal or other professional advice. The applicability of this material is not intended to be relied on as a complete and accurate interpretation of the law for any person or entity. Liberty Tree Financial Services, Inc. accepts no responsibility for the accuracy or completeness of this material and you use it at your own risk.*