

# FACTA “Red Flag Rules” Compliance

**Identity Theft** - it's becoming an increasingly common and complex crime with a very real economic impact on your company, employees and customers. Millions of sensitive records are lost or stolen from databases across the country every year and statistically at least one in five of your customers and employees will become a victim. It's safe to say that **identity theft costs companies and consumers billions of dollars each year.**

## What is FACTA?

The **Fair and Accurate Credit Transaction Act of 2003** (FACTA) was issued by Congress and signed into law to help consumers fight the growing crime of identity theft.

Section 114 of FACTA, commonly referred to as the “Red Flag” provision, requires that the Federal Trade Commission and Federal Banking Agencies issue identity theft program guidelines and regulations, to which financial institutions and creditor organizations must then comply by a specified date (ref. below).

The following agencies jointly issued the final rules and guidelines:

- Federal Trade Commission
- Federal Deposit Insurance Corporation
- Federal Reserve System
- Department of the Treasury
- Treasury Office of Thrift Supervision
- Treasury Comptroller of Currency
- National Credit Union Administration

The final rule can be found at the following Web site link:

<http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

## What is required to be FACTA-compliant?

FACTA requires financial institutions and creditor organizations to develop, document and implement a **comprehensive identity theft program that includes information security policies, procedures and incident response plans** covering personal (e.g., consumer, customer, patient) information. The objective of this program is to mitigate identity theft risks through the effective prevention, detection and management of “Red Flag” incidents (ref. below).

The program must be administered by a board of directors or senior management and be periodically (min. annual) reviewed, updated and confirmed.

The program must also ensure that relevant vendors are compliant.

## When does FACTA take effect (and what is the deadline for compliance)?

The final FACTA regulations were put into place November 2007. Full compliance was originally set at **November 1, 2008**. However, in an announcement dated October 22, 2008, the FTC explained that it will not enforce the Red Flag Rules until **May 1, 2009**, effectively giving companies under its jurisdiction an extension of six months to comply. This announcement does not affect companies subject to the enforcement authority of federal agencies other than the FTC.

## How can Perkins & Company help?

Mandates like FACTA can detract your IT resources from operations and critical initiatives as your company strives to manage – and ultimately benefit from – fast-approaching deadlines and ongoing compliance. At the same time, practical IT governance, risk management and compliance have never been more critical to your business' success. It's an important balance, and that's where Perkins Risk Management practice comes in.

We can help you practically implement the right “Red Flag” program by working with your team to:

- completely understand workflow and systems supporting relevant account activity and information classes;
- assess information risks (on and off systems);
- create a red flag program (documented policies, procedures, response plans) that meet red flag compliance requirements;
- confirm vendor compliance; and
- educate/help drive policy awareness internally.

# FACTA “Red Flags”

## What are the “Red Flags?”

FACTA requires that identity theft programs prevent, detect and respond to “Red Flags”: patterns, practices and/or activities that warn of potential identity theft.

Since every business is different, it is essentially impossible to provide a comprehensive list of Red Flags. However, the **FTC has issued guidelines for businesses to consider when writing their programs; these include:**

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personally identifying information, such as a suspicious address
- Unusual use of – or suspicious activity relating to – a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts

## Who is required to comply with FACTA?

FACTA Red Flag Rules apply to financial institutions and creditors with covered accounts. According to the regulations, a covered account is:

- an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; or
- any other account for which there is a foreseeable risk of identity theft.

For example, a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.

**At a minimum, industries subject to FACTA regulations include:**

- banks;
- finance companies;
- automobile dealers;
- mortgage brokers;
- utility companies; and
- telecommunication companies.

The regulations can also be interpreted to include:

- insurance companies and brokers;
- credit/finance companies;
- hospitals and other health care companies;
- municipal utility districts;
- legal service providers;
- leasing organizations;
- and others.

## What is the cost of non-compliance?

Financial institutions covered by the FACTA Red Flag Rules are subject to federal banking regulator oversight, which may include penalties consistent with the regulatory authority. For non-federally-regulated creditors, the Federal Trade Commission (FTC) provides oversight and may impose civil penalties of up to \$2,500 per infraction. In either case, the non-compliant organization must also consider other impacts like brand damage, customer loss and/or legal costs (e.g., civil action, class action law suits).

Senior management is ultimately responsible for – i.e., vulnerable for lack of – implementation, administration and periodic program review.

## Why Perkins?

Perkins clients benefit from our experience. . . Perkins consultants have performed IT risk management and compliance services for companies across a variety of industries. And, as a large, local accounting and business advisory firm, we work with you to understand your information risks in the context of your industry and business objectives.

Looking for experienced information risk and compliance help?

**Please contact us:**

Sue Markovitz  
Perkins & Company, P.C.  
1211 SW Fifth Avenue  
Suite 1000  
Portland, Oregon 97204  
503.221.0336  
smarkovitz@perkinsaccounting.com  
www.perkinsaccounting.com



**PERKINS & CO**

503.221.0336

www.perkinsaccounting.com