

Identity Theft Loss Prevention, LLC Statement on the Red Flag Clarification Act of 2010

“On December 18, 2010, President Obama signed the Red Flag Clarification of 2010. The bill amended the Red Flags Rule of the Fair and Accurate Credit Transactions Act of 2003.”

In October 2007, the Joint Committee of the Office of the Comptroller of Currency (OCC), the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), and the Federal Trade Commission passed final legislation for sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). They are known as Red Flag Regulations and Guidelines.

The Red Flag Regulations and Guidelines require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. The effective date was January 1, 2008.

The first enforcement date was set for May 1, 2008. Due to disagreements on the definition of what a “creditor” is, as defined by the Equal Credit Opportunity Act, many organizations did not understand their obligation to comply. The enforcement date was changed several times with the final deadline falling on December 31, 2010.

In an attempt by Congress to clearly define who is considered a creditor under the Red Flags Rule, the Red Flag Clarification Act of 2010 was signed. The Act changes specific elements under the definition of creditor. The intent seemed to be that by removing certain activities describing any person (creditor), who grants rights to a debtor to defer payment of debt or to incur debt and defer its payment, or to purchase property or services and defer payment therefore (credit), that certain industries might be excluded from compliance.

Since each organization’s information and account management activity is different, it raises many questions about excluding any industry in its entirety from the regulations. Each organization is encouraged to assess its own practices to determine if it has to comply with regulations specific to the Red Flags Rule. Furthermore, it is imperative for stakeholders in any organization to fully understand their liability under a myriad of existing laws, regulations, and perhaps most importantly to the consumer.

In spite of these current changes to one piece of legislation, it is important not to get distracted from the real issue at hand. An untold truth is that the “exposure” of confidential and sensitive information places any person, business, school, government agency, or other organization that collects or maintains it at great risk. Once these identifiers are exposed to an unauthorized third party, not only is the impact devastating to the affected entity, but the board, executives, and employees may be held vicariously liable by law for the manner in which the information is used.

Thinking of all of the practices in your organization related to information can bring many questions to mind. At what points in process is there potential exposure? What assessment has been done? Did the assessment bring all of the necessary concerns into scope? Were policies and procedures properly drafted? Is employee, vendor, or consumer behavior leaving you exposed? What is the *total* impact of an exposure on your organization? Can your personal assets weather the vicarious liability of an information loss?

The only effective approach to identify and limit information exposure is through an enterprise risk management process. This requires partnering with a third-party expert to bring your information exposure issues into scope. It must assess the organization in its entirety and then facilitate appropriate practices to close the gaps. Well-drafted policies and procedures (focused on the appropriate scope of information) act as rules of engagement for daily operations. Other key elements include implementation, training, and proper response measures.

The Red Flags Rule is only one regulation that is focused on information *usage*. When an employee of your organization allows the wrong person to transact on accounts there is still considerable liability even if you are determined to be exempt from compliance with the Red Flags Rule. There are additional obligations under other existing legislation for *privacy, security, notification and response*.

The greatest obligation that you have is to the consumer. They are the ultimate judge of your actions. Consumers will choose not to conduct business where they do not feel safe. Laws are written to protect them. In class action lawsuits where an exposure becomes identity theft, your organization, and possibly you personally, will pay them. So the real question now becomes, not do you have to comply with the Red Flags Rule, but can you *prove* that you have made a “reasonable effort” to detect, prevent, and mitigate information exposure?

For more information, please contact Tom Glanville or Frank R. Mitchell of Identity Theft Loss Prevention, LLC at info@idtlp.com.