



THE RED FLAGS RULE

Identity Theft Business Solutions, Inc.



Protecting Businesses and Families across North America

The Identity Theft Risk Assessment

Risk is the possibility of something adverse happening. The process of identity theft risk management is identifying risks related to sensitive and non-public information, assessing the likelihood of their occurrence, and then taking steps to reduce the risk to an acceptable level. The identity theft risk assessment process begins with determining the area(s) to be assessed, identifying the type(s) of information circulating the area(s), reviewing the day-to-day business operations that may put information at risk and then making formal recommendations of the controls needed to lower the likelihood of an identity theft occurrence.

The primary function of identity theft risk management is the identification of appropriate controls. The goal of controls is not to have 100% security; total control would mean zero productivity for your company. Controls must never lose sight of your objective or mission and should be easy to implement.

Performing a risk assessment is the first step in identifying vulnerable areas but that alone will not reduce the risk of identity theft. Employees have a huge role to play in detecting, preventing and responding to signs or “Red Flags” associated with identity theft. Once risks or vulnerabilities are identified, the recommended controls are written into an Identity Theft Prevention Program (ITPP) policy. The policy must then be submitted to your Board for approval. Upon Board approval, the success of your ITPP depends on one very critical factor, **staff training**. Training staff to adhere to the policies and procedures within your Program is the most critical step in a successful Identity Theft Prevention Program. If your staff has not been trained on the policies within your Program, it is highly unlikely that they will adhere to your new policy or are even aware that your policy exists.

In addition, your company’s security practices depend on the people who implement them, including independent agents and service providers. Before you outsource or subcontract any part of your business functions, investigate the company’s data security practices and compare their standards to yours. If possible visit their facilities. Select service providers that are “qualified” to maintain appropriate safeguards and make sure your contract requires them to adhere to the identity theft privacy laws.

An annual update to your Program is the minimum requirement to ensure that you keep current with new identity theft risks. Factor in your own identity theft experiences, new methods of detection, changes in accounts you offer, changes in your business model or arrangements with service providers. Include your staff in the annual update process. Conducting periodic risk assessments will help you determine if there have been changes in your process for handling sensitive information. Include the risk assessment and staff training in your annual update process, together they are the best defense against identity theft and data breaches. .



Protecting Businesses and Families across North America

Scope of Work

Identity Theft Business Solutions (IDTBS) will provide the following to the [COMPANY NAME HERE] as a part of their **Identity Theft Prevention Program**.

- **Information Security Coordinator (ISC)** designee, whose responsibilities will include monitoring the effectiveness of the Identity Theft Prevention Program and working with the CITRMS agent to review and update your Program when needed.
- **Comprehensive Risk Assessment (R/A)** of data security practices as well as assessment of information security during day-to-day business operations. The Risk Assessment will identify current Red Flags and practices that leave information vulnerable within your workplace. The risk assessment will also assist in the development of appropriate policies and procedures and training points for staff.
- **Policies and Procedures** that governs the handling, storage, and disposal of sensitive and non-public information in the workplace. This policy is intended to become a blueprint for staff and give them a heightened sense of awareness of identity theft as well as step-by-step procedures to follow when presented with situations where there may be Red Flags. The employee **Confidentiality Agreement**, which each employee will sign, serves to protect the company from employee related theft of sensitive information and act as proof that your staff has been trained on the Identity Theft Prevention Program.
- **Mandatory Employee Training** to raise awareness of the issues of identity theft as well as instruct on policies and procedures for handling sensitive and confidential information.
- **Qualify Service Providers** in accordance with the Federal Trade Commission recommendations. Service providers should handle customer information as carefully as you do. If your service providers do not have a documented Identity Theft Prevention Program in place, they will be required to sign an Indemnification document, which holds your company harmless for any data security breaches or theft caused by the service provider or other third party vendors.
- **Annual Review/Training Updates** of the Identity Theft Prevention Program, which will include a review of data security practices and day-to-day business operations. In the event of changes in the business infrastructure, staff turnover or locations, more frequent reviews/updates are recommended. Updates to the current Identity Theft Prevention Program Policy as well as staff training updates will be performed at this time. Annual updates are necessary to review the effectiveness of your ITPP, to address any newly identified Red Flags and to inform management and staff of any changes in the Federal Privacy Laws,



Protecting Businesses and Families across North America

About

IDentity Theft Business Solutions, Inc.

Identity Theft Business Solutions (IDTBS) is an industry pioneer and top-tier risk management firm that provides compliance solutions to companies throughout the U.S. IDTBS is a privately held company, founded in July of 2004 by Mark G. Brown, Sr. As a respected part of the Information Technology & Security industry for over twenty (20) years, Mr. Brown followed his passion for information security even further and developed a business model that not only addressed computer security issues but also addressed the human aspects of data vulnerability.

In addition to working with local government agencies, Sheriff's departments, and private corporations, IDTBS participates in the Federal Trade Commission's 'National Education Campaign', an effort put forth to educate and assist businesses with implementation of the requirements necessary to Deter, Detect and Defend against identity theft.

Risk management services include, data security & business operation risk assessment(s), employee training(s), policy and procedures, contractor/service provider qualification and review, preventative/reactive data breach assistance and annual updates.

As a leader in identity theft prevention and compliance solutions, our Certified Identity Theft Risk Management Specialist (CITRMS) help businesses identify and manage risks associated with identity theft and data loss. CITRMS agents are certified by The Institute of Fraud Risk Management (TIFRM), in conjunction with the Institute of Consumer Financial Education (ICFE). Our CITRMS agents are also active members of the International Association of Privacy Professionals (IAPP). These highly qualified professionals have trained and protected thousands of companies and tens of thousands of individuals from identity theft and fraud related issues. Our customized Programs have saved companies potentially millions of dollars in fines, penalties and lawsuits associated with being out of compliance with the identity theft Federal Privacy Laws.

IDTBS will develop and implement a customized Identity Theft Prevention Program which meets the requirements necessary to help your company adhere to new Federal Privacy Laws. In addition, pursuant to the Federal Trade Commission's Red Flags Rule, Section 114 of the Fair and Accurate Credit Transaction Act of 2003(FACTA), this program puts measures in place that meet guidelines set forth in the Rule.

IDentity Theft Business Solutions, Inc.

700 Old Dixie Hwy, Ste. 108

Lake Park, FL 33403

Office: (561) 869-4495

Fax: (561) 713-2743

Website: www.idtbs.com

Email: support@idtbs.com