Beware of 'Red Flags': What Must Your Business Do to Protect Customers from Identity Theft?

July 3, 2013

State and federal laws, including Federal Trade Commission regulations that were revised in late 2012, require certain businesses to play an active role in the identification, mitigation, and prevention of identity theft. Does your business have any legal obligation to combat identity theft? The answer may be "yes."

Despite growing awareness of the problem, identity theft continues to occur with increasing frequency and losses continue to rise. For years, identity theft has been the most common complaint received by the Federal Trade Commission ("FTC"). The FTC recently reported that of the more than 2,000,000 complaints it received in 2012, nearly 20% related to identity theft, including the misuse of personal information such as a social security, credit, or bank account number to commit fraud or theft.

Clearly this is bad news for individual victims, but does your business have any legal obligation to combat identity theft? ***The answer may be "yes."*** Under a smattering of state and federal statutes and regulations, businesses are increasingly being drafted by the government to fight in the war against identity theft.

FTC Red Flags Rule

FTC regulations addressing identity theft were revised in late 2012 ("Regulations"). A portion of the Regulations, commonly called the "Red Flags Rule" because it attempts to point out indicators of identity theft, requires certain businesses to play an active role in the identification, mitigation, and prevention of identity theft. "Identity theft" means a fraud committed or attempted using another person's information without authority to do so. All "creditors" with "covered accounts" must adopt and implement a written identity theft prevention program addressing identity theft "red flags."

Is Your Company a "Creditor"?

Determining whether your company is a "creditor" under the Red Flags Rule is a somewhat complex analysis. The term includes any business entity that regularly extends credit in the ordinary course of its business to individual consumers, as opposed to credit for business purposes. According to recent guidance from the FTC, merely allowing deferral of payment by your customers does not automatically make your company a "creditor," although it remains a factor in the analysis. However, if your business obtains consumer credit reports or provides credit information to credit reporting companies with regard to individual consumers, it is very likely a creditor.

What is a "Covered Account"?

A "covered account" is any credit account used primarily for personal, family, or household purposes and which permits multiple payments or transactions, *or* any account for which there is a reasonably foreseeable risk of identity theft (even if it is a commercial account). These broad definitions mean that the term "covered account" includes far more than just a credit card account. For example, even some leases are considered covered accounts.

The "Red Flags Rule" Requirements

If the FTC's Red Flags Rule applies to your business, you must adopt and implement a written program with at least four key features:

- Identification. Your program must identify "red flags" (that is, warning signs) indicative of identity theft when they occur. The Red Flags Rule lists 26 potential red flags. You must create a customized list of potential red flags specific to your own business using the 26 potential red flags as a guide.
- Detection. Once you have identified the red flags applicable to your business, your program must include procedures for detecting them. The detection procedures may be tailored to your business. For example, if your business is large with millions of customers, you may need a much more robust detection program than a small business where each customer is personally known to your employees. If your business handles large dollar amounts and very sensitive data, you should have a more vigorous detection program than a business that handles small amounts and less sensitive categories of data.
- Response. Next, your program must establish response procedures designed to effectively prevent or mitigate the occurrence of identity theft. All responses should be commensurate with the risk detected. The Red Flags Rule provides some guidance as to acceptable responses.
- Revision. Your program, once adopted, must not remain static forever. Identity theft methods are dynamic, adapting over time, and, therefore, your policies must be reviewed periodically and systematically to ensure they remain effective.

The Red Flags Rule also requires that your employees be trained on the program to ensure it is properly implemented.

FTC Address Discrepancy Rule

Somewhat related to the Red Flags Rule, the FTC's Address Discrepancy Rule requires regular users of consumer credit reports to implement policies and procedures to respond to discrepancies in reported consumer addresses. This program can be integrated with your Red Flags Rule program. If your business requests a consumer credit report, it will receive a Notice of Address Discrepancy if the address your business has given is substantially different from the address on file with the credit bureaus. In an effort to enlist the help of businesses in preventing identity theft, the Address Discrepancy Rule requires your business to respond appropriately to an address discrepancy rather than ignore it. As is the case under the Red Flags Rule, your business has the flexibility to develop and implement a policy suitable to your business model.

State Identity Theft Laws

In addition to the federal rules described above, many states have their own identity theft laws, data security breach laws, or other "privacy" laws designed to prevent or mitigate the unauthorized or unintentional disclosure of customer information by businesses.

The North Carolina Identity Theft Protection Act ("ITPA") is an example of a multi-faceted state statute intended to address identity theft. The ITPA requires social security numbers ("SSN") to be kept confidential and restricts their use by businesses. For example, businesses are generally not allowed to require a North Carolina consumer to put his or her SSN on a card or transmit it over the Internet. The ITPA also requires businesses to dispose of North Carolina residents' personal information in ways that protect against unauthorized access, such as by secure shredding. Simply placing documents (or data storage media) containing personal information in a trashcan to be dumped in a landfill can subject your business to liability.

The ITPA requires businesses that experience certain security breaches in which North Carolina consumers' personal information may have been compromised to notify the North Carolina Attorney General and the potentially affected consumers. Similarly, the ITPA makes it unlawful to publicize a North Carolina consumer's personal information. Therefore, the ITPA approaches identity theft in a number of ways, each of which must be observed by businesses operating in North Carolina. A violation of certain parts of the ITPA by a business is an unfair trade practice, the penalties for which can be quite costly.

Other states have similar statutes and regulations addressing a business's responsibility to prevent or limit identity theft. If your business has out-of-state customers, it is important for you to determine if your business must legally comply with the laws of the customers' state and, if so, to determine what duties that state's law imposes. Perhaps no state has stronger consumer protections in this area than California. Any company doing business with California residents is well-advised to become familiar with California's various consumer protection laws relating to identity theft, information security, and privacy.

In addition to the statutory and regulatory requirements imposed on businesses, there is risk of civil liability associated with customer identity theft. If your business fails to adequately protect against, or respond to, a data breach or identity theft, you may find your business sued for damages suffered by your customers.

Conclusion

As recent high-profile examples have shown, a business's failure to prevent or respond appropriately to identity theft or a data breach can result in massive liability from a number of sources. One of the best steps your company can take to protect itself prior to a problem arising is to create, adopt, and implement a well-conceived identity theft plan. Not only will such a plan prevent potential identity theft, it may also help limit your company's losses in the event a problem does occur. Your business is well-advised to act promptly to protect your customers—and therefore itself—from the growing threat of identity theft.

--