LINDABURY

McCormick, Estabrook & Cooper, P.C.

Attorneys at Law

Cybersecurity & Data Privacy

Customer Data, FTC Red Flags Rules & Your Business

Identity theft is an area of major concern for consumers and businesses alike. Roughly nine million individuals in the U.S. can expect to have their identity stolen each year. With just a few items of personal information (such as the name, social security number, and the date of birth of an individual) a cyber-criminal can potentially drain existing accounts or open new credit card accounts with devastating consequences for the unwitting consumer's credit ratings and future path in life.

If your business has been lax in protecting the privacy of such personal information in its possession, you may be inviting your own devastating consequences:

- lawsuits by individuals experiencing identity theft as a result of your lax procedures
- regulatory enforcement actions
- damage to your business reputation and loss of trust by your customers

FTC Red Flags Rule

The Red Flags Rule, issued by the Federal Trade Commission ("FTC"), requires financial institutions and creditors with covered accounts (as defined in the Red Flags Rule) to develop a written program that identifies and detects the relevant warning signs, or red flags, of identity theft. Red flags can include:

- Unusual account activity
- Fraud alerts on a consumer report
- Attempted use of suspicious account application documents

The Red Flags Rule's definition of a "creditor" is broad, and includes any entity that regularly extends or renews credit (including entities that regularly permit deferred payment for goods or services). However, the Red Flags Program Clarification Act of 2010 limits the Rule's application to those creditors that regularly and in the ordinary course of business:

- Obtain or use consumer reports directly or indirectly with a credit transaction
- Furnish information to certain consumer reporting agencies in connection with a credit transaction
- Advance funds to or on behalf of a person, based on the person's obligation to repay the funds from a specific property pledged by or on behalf of that person

The FTC's Red Flags Rule also requires that the identity theft program must be approved by the covered entity's board of directors, and should be reflective of policies and procedures that are appropriate to the covered entity based on suggested guidelines established by the FTC.

SEC & CFTC Red Flags Rules

In April 2013 the Securities and Exchange Commission ("SEC") and Commodity Futures Trading Commission ("CFTC") published their own Red Flags Rules requiring financial institutions and creditors with covered accounts to develop and implement a written identity theft prevention programs to detect, prevent, and mitigate identity theft. The SEC and CFTC rules are similar to the FTC's Red Flags Rule, but transfer jurisdiction from the FTC to the SEC and CFTC for entities subject to their regulatory oversight.

The written identity theft prevention program must include reasonable policies and procedures appropriate to the size and complexity of the financial institution or creditor, such as:

- Identify relevant red flags for the covered entity
- Detect red flags
- Respond to red flags
- Ensure the program is updated periodically