

Identity Theft Red Flag Rules Alert: You May Be Required to Comply!¹

If you offer credit or payment plans to consumers, or you allow consumers to pay over time in installments, you are considered a Creditor or a Financial Institution under the Identity Theft Red Flags Rules (the “Rules”), and you must establish a written Identity Theft Red Flag Rules Program (“Program”) by May 1, 2009. The Rules apply to financial institutions and non-financial institutions alike, including non-profits, government entities, and other entities that allow consumers to pay over time, as diverse as utility companies, charities, and healthcare providers. All such entities are required to establish and maintain a written Program although the details will vary depending on such factors as the size of entity, the kinds of consumer accounts the entity maintains, and the potential risk of identity theft. The Rules do not apply to entities which accept payment by credit card only on a single transaction basis.

What are the Red Flag Rules?

The Rules were issued by the Federal Trade Commission (“FTC”), the federal banking regulatory agencies and the National Credit Union Administration (“NCUA”) pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”), and are aimed at detecting, preventing, and mitigating identity theft. The compliance deadline originally was November 1, 2008, although the FTC delayed its enforcement until May 1, 2009. This was due in part to the fact that many entities were unaware that they are regarded as creditors or financial institutions under the Rules, especially because many of the affected entities previously have not been required to comply with FTC's rules in other contexts. The deadline was not changed for entities subject to the oversight of the other agencies (for example, banks) and therefore such entities must already have their Programs in place.

What is required?

Entities must create and institute a written Program that is appropriate to their size and operations which identifies and detects patterns, practices and specific forms of activity (or “red flags”) that indicate the possible existence of identity theft. The Rules provide an extensive list of potential red flags for entities to use in identifying potential red flags in their organizations, for example, the attempted use of a photocopied driver’s license as proof of identification, unusual account activity, or a suspicious address change request.

However, these are provided as illustration and the actual red flags that an entity identifies will depend on such factors as the size of the entity and the kinds of consumer accounts the entity maintains.

¹ © 2009 Isaacson Rosenbaum P.C. Prepared by Susan E. Gindin. Susan is Of Counsel to the firm and specializes in intellectual property and online law, data privacy and security, advertising and contest law.

The Program must also provide procedures for detecting red flags if they occur, and it must plan for appropriate responses to prevent and mitigate identity theft if a red flag is detected. For example, in addition to monitoring an account for evidence of identity theft, the entity may find it appropriate to contact the consumer, change passwords, close an existing account, or notify law enforcement. The response will depend on the circumstances but must be well-considered.

Other requirements are that the Program include staff training, and provide oversight for any service providers who have access to consumer information.

Another key part of the Program is a plan to update the Program periodically, for example, to determine whether the Program is working, to address new means of identity theft, and to address any new risks related to changes in the entity's operations or the type of accounts offered.

Once an entity has analyzed its accounts which include consumer information, identified potential red flags, provided procedures for detecting red flags, proposed responses in order to prevent or mitigate the occurrence of identity theft, provided for training of staff and oversight of any service providers, and provided a plan for periodic updating of the Program, the entity must document the Program in writing.

Board Approval and Oversight

The initial written Program must be approved by the board of directors or a committee of the board (or by senior management if the entity has no board of directors), and the board, board committee or designated senior management employee must oversee the implementation and administration of the Program, review reports regarding the Program (which must be prepared by entity staff annually), and approve significant changes to the Program.

The initial written Program, reports, and any decisions made pursuant to the Program must be well-documented. For example, if the entity identifies a potential identity theft red flag, and after review of the circumstances, the entity determines there is little risk of identity theft and decides to take no further action, the entity should fully document its review and determinations in response to the occurrence of the red flag. In addition to raising the profile of the Program within the entity, it will be an important paper trail in the event of FTC or other governmental scrutiny.

The current penalties for failure to comply with the Rules include fines of up to \$2,500 per violation, and regulatory enforcement actions. However, there is an added risk of harm to the entity's reputation. In addition, the Rules will likely become a standard of care for appropriate handling of consumer information, and the entity's well-documented and compliant Program will be helpful if the entity is ever implicated in the identity theft of one of its account holders.

If you need assistance with creation, implementation, documentation, staff training, or any part of your Red Flags Program, contact Susan Gindin at 303-256-7046 or sgindin@ir-law.com. Susan has been practicing in the area of identity theft and data privacy law for over thirteen years. Also, look for Susan's upcoming article on data breach laws and their implications for your operations.