

October 2008

**Contacts****[Lisa J. Sotto](#)**

200 Park Avenue  
New York, NY 10166  
(212) 309-1223  
[lsotto@hunton.com](mailto:lsotto@hunton.com)

**[Boris Segalis](#)**

200 Park Avenue  
New York, NY 10166  
(212) 309-1289  
[bsegalis@hunton.com](mailto:bsegalis@hunton.com)

**Additional Lawyers**

[Cédric Burton](#)

[James A. Harvey](#)

[Jörg Hladjk](#)

[Natalie Hunt](#)

[Elizabeth H. Johnson](#)

[Christopher Kuner](#)

[Ryan P. Logan](#)

[Manuel E. Maisog](#)

[Melinda McLellan](#)

[Randall S. Parks](#)

[Olivier Proust](#)

[Aaron P. Simpson](#)

[Rachel M. St. John](#)

[Bridget C. Treacy](#)

Mason Weisz

[John W. Woods, Jr.](#)

**Centre for Information****Policy Leadership**

[Martin E. Abrams\\*](#)

[Paula J. Bruening](#)

[Fred H. Cate](#)

[Orson Swindle\\*](#)

\*Not a lawyer

**Red Flags Rule Compliance Deadline Approaching**

November 1, 2008 is the deadline for compliance with the Identity Theft Red Flags and Address Discrepancies Rule (the "Red Flags Rule" or "Rule"). The Rule was promulgated jointly by the Federal Trade Commission (the "FTC") and various bank regulatory agencies pursuant to Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (the "FACT Act"). The Rule applies to financial institutions, creditors, users of consumer reports and credit and debit card issuers. According to the FTC, "a very large number of ... entities across almost every industry" may be subject to the Rule.

The Rule requires financial institutions and creditors that offer or maintain certain accounts to develop and implement a written identity theft prevention program. In addition, it requires users of consumer reports to implement procedures for handling notices of address discrepancy that they receive from consumer reporting agencies ("CRAs"). Finally, credit and debit card issuers are required to implement procedures for assessing the validity of change of address notifications.

**Identity Theft Prevention Program**

The primary focus of the Red Flags Rule is the requirement to implement an identity theft prevention program designed to detect, prevent and mitigate identity theft. The Rule does not articulate specific requirements for the program's form or content, but instead sets forth the process

that businesses must follow in developing, implementing and administering the program. This process may be challenging and time-consuming, especially for businesses that previously have not taken a comprehensive approach to combating identity theft.

The identity theft prevention program requirements apply to two categories of businesses: (i) financial institutions that hold consumer accounts from which account holders can withdraw or direct funds for payment to third parties, and (ii) "creditors," which are defined as businesses that allow customers to defer payment of debt or payment for purchases of property or services. Car dealers, utilities, retailers, cellular phone carriers, hospitals and mortgage brokers are just a few examples of creditors that may be within the scope of the Rule. The Rule also affects service providers to financial institutions and creditors because it requires relevant businesses to ensure that their service providers perform their duties in accordance with policies and procedures designed to detect, prevent and mitigate identity theft.

Not every financial institution or creditor is subject to the provision requiring the establishment of an identity theft prevention program. Rather, this requirement applies only to entities that offer or maintain (i) consumer accounts that involve multiple transactions or (ii) other accounts that are

associated with a reasonable risk of harm from identity theft.

Entities that are subject to the Red Flags Rule must develop programs that are tailored to the organizations' size and complexity and the nature of their operations. The Rule requires businesses to (i) identify relevant patterns, practices and activities that indicate the possible existence of identity theft (*i.e.*, Red Flags), and (ii) develop methods for detecting and responding to those Red Flags. There is additional guidance in the Rule on developing, implementing and administering an identity theft prevention program, including examples of Red Flags and suggested detection and response methods. Note, however, that the FTC and bank regulatory agencies have specifically cautioned businesses against using the guidelines as a substitute for their own efforts to identify relevant Red Flags and develop appropriate detection and response methods. Businesses are required to document both the program and the steps they take to develop it. Following the initial approval and implementation, businesses must periodically evaluate the program's effectiveness and appropriately update it to reflect their own experiences with identity theft issues as well as changes in relevant business arrangements and known methods of identity theft.

#### **Notices of Address Discrepancy**

The Red Flags Rule also requires businesses that use consumer reports to implement reasonable policies

and procedures for handling notices of address discrepancy. A consumer reporting agency issues such a notice when the address provided in a request for a consumer report substantially differs (as determined by the CRA) from addresses the agency has on file for the relevant individual. Responding to a notice of address discrepancy requires businesses to (i) verify that the consumer report relates to the individual about whom the report was requested, and (ii) confirm the individual's accurate address. In addition, under certain circumstances, the relevant individual's accurate address must be reported to the CRA that issued the notice. This provision may apply to employers, insurance companies, debt collectors, lenders and other users of consumer reports. Notably, some businesses have taken the position that this provision applies only to notices issued by the three nationwide credit reporting agencies (Equifax, Experian and TransUnion) in connection with requests for credit reports (as opposed to, for example, background check reports provided by agencies such as ChoicePoint).

#### **Notifications of Change of Address**

The Rule requires issuers of credit or debit cards to establish reasonable policies and procedures for assessing the validity of change of address notifications. When a notification is followed within thirty days by a request for an additional or replacement payment card, the Rule prohibits issuers from providing the customer with a card until the change of address is verified.

#### **Enforcement**

The FTC has the primary responsibility for enforcing the Red Flags Rule. It will oversee implementation of the Rule by all relevant businesses that are not regulated by the various banking agencies (the OCC, the Federal Reserve, the FDIC, the OTS and the NCUA). Notably, because the SEC does not have Rulemaking authority under Section 114 of the FACT Act, the FTC will also enforce the Rule with respect to investment companies and other entities that are ordinarily regulated by the SEC.

Enforcement will focus initially on verifying that businesses followed the process set forth in the Rule to develop their identity theft prevention programs. Subsequent agency reviews may focus on the overall effectiveness of the programs and their administration, including periodic assessments and compliance reports. We expect the FTC and banking agencies to provide additional guidance on enforcement in FAQs and examination guidelines to be published this fall.

#### **We Can Help**

Many businesses are facing significant challenges in understanding and complying with the Red Flags Rule's complex requirements. Hunton & Williams' Privacy and Information Management practice has been advising clients in myriad industries on compliance with the Rule. If you would like assistance with the Red Flags Rule, please contact us.

© 2008 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.