

# NICOLAI LAW GROUP, P.C.

## BUSINESS LAW & LITIGATION

Paul Peter Nicolai, Esq.  
Also Admitted in New York,  
Connecticut &  
Washington, D.C.  
Fellow, American Bar Foundation  
Direct Dial Extension 222  
E-MAIL Address:  
PAUL.NICOLAI@NICLAWGRP.COM

Tarbell-Watters Building  
146 Chestnut Street  
Springfield, Massachusetts 01103-1539  
Internet: WWW.NICLAWGRP.COM  
Telephone: 413-272-2000  
Facsimile: 413-272-2010

TO: Clients & Interested Parties

FROM: NLG Professional Staff

DATE: March 1, 2009

## RE: Red Flags Regulations

The Red Flags regulations are a major privacy initiative. This memorandum explains the regulations, their background and the compliance measures affected organizations need to prepare for. On May 1, 2009, US financial institutions and creditors will be required to comply with these regulations adopted by the Federal Trade Commission ("FTC") and US financial institution regulators. The regulations require each to develop and implement programs designed to detect, prevent and mitigate the effects of identity theft.

### IDENTITY THEFT

Identity theft is fraudulently using an individual's personal information to open financial accounts, incur debts or transact business in the victim's name. To commit identity theft, a person must obtain another person's personal information and successfully use that information to open an unauthorized account or make unauthorized charges against an existing account. Identity theft was made a federal crime in 1998.

For existing account fraud, the thief gets the personal information needed to charge purchases against a victim's account and uses it to get goods or services charged to the victim's account. For new account fraud, it is usually more complicated. Before extending credit to a new customer, businesses usually confirm the applicant is a good credit risk. That needs information about the applicant's personal financial history - information an impostor typically will not have.

The problem is creditors generally do not ask the applicant to supply all the information needed to assess credit. Instead, they collect the applicant's detailed financial history from credit reporting agencies. To do this, the creditor only needs a few items of personal information from the applicant. When submitted to a credit-reporting agency, the agency will match that information with its records and give the file to the creditor. If the creditor is satisfied, it usually opens a new account giving the applicant credit. The thief gets the goods and the victim gets the bills.

---

**NICOLAI LAW GROUP, P.C. • BUSINESS LAW & LITIGATION • 413-272-2000**

This material is provided for information and education purposes to clients and others who may be interested in the subject matter. It is not legal advice or a legal opinion that can only be given on specific facts.

Preventing identity theft is a multi-step process. The first and most effective step is to keep unauthorized persons from getting personal information. If that fails, creditors and credit reporting agencies can prevent the successful misuse of stolen data by requiring more information from new account applicants and those trying to make charges against existing accounts, or by taking steps to verify the identities of persons whose attempts to use or establish credit seem questionable. Finally, if all those efforts fail and identity theft is successful, businesses can soften the impact by forgiving unauthorized charges.

US Creditors and financial institutions have taken steps to make identity theft more difficult. Better record management and information security have improved stored personal information security. The Payment Card Industry Data Security Standard has put uniform data security measures on payment card processors and users. Existing account fraud has been made more difficult by payment cards that include security codes only someone with the card can provide. Payment card issuers have implemented sophisticated programs that spot suspect transactions and trigger notification.

The law has also moved to reduce the incidence and impact of identity theft. A number of state, federal and foreign laws require organizations that maintain personal information to protect it from unauthorized access, disclosure and use. These obligations are intended to keep identity thieves from acquiring the personal information of others in the first place. In 2003 California enacted the first data security breach notification law. Those laws, now in force in at practically all states, give individuals notice when their personal data may have been compromised so they can take action to minimize identity theft. We also have “credit freeze” laws which give consumers the right to block access to their credit reports by new creditors.

Another step was the adoption, under the USA Patriot Act, of Customer Identification Program (“CIP”) regulations. They require all banks, savings associations, credit unions and some other banks to implement procedures to verify the identity of each customer. When individuals open new accounts, banks must get the person's name, date of birth and address. The program also must have procedures for verifying customer identity within a reasonable time after the account is opened, like contacting the customer or getting a report from a credit-reporting agency.

These still leave a gap in the protections against identity theft. They do not necessarily identify all the measures creditors and financial institutions should take to spot and respond to questionable credit applications likely to be the work of identity thieves. The Red Flags regulations impose new legal obligations on financial institutions and businesses of all kinds that extend credit to consumers to try to close this gap. Not later than May 1, 2009, all such businesses must have in place a program that identifies and provides effective means for dealing with suspicious circumstances that suggest a threat of identity theft to its’ customers.

## **REQUIREMENTS**

The Red Flags regulations are amendments to the Fair Credit Reporting Act. However, they have a broader impact than previous regulations that apply mostly to consumer reporting agencies. The new regulations must be observed by two wide categories of businesses: “financial institutions” and “creditors.”

Financial institutions include any bank, savings and loan association, credit union or any other person that directly or indirectly holds a transaction account belonging to a consumer. A creditor includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility com-

panies, and telecommunications companies. Essentially, anyone that furnishes goods or services on credit is a creditor.

The Regulations require affected businesses to take a wide range of measures, including policies aimed at changes of address and address discrepancies and development of comprehensive identity theft prevention programs.

### Duties of Card Issuers Regarding Changes of Address

Some of the Red Flags obligations are imposed specifically on debit and credit card issuers. They must be prepared to deal with cases where a change of address notice is followed, within 30 days or less, by a request for an additional or replacement card for the same account. The issuer may not issue that card until it has notified the cardholder of the request at the former address or other means previously agreed to. The issuer also must give the cardholder a means of promptly reporting incorrect address changes or otherwise assess the validity of the change of address in accordance with the policies and procedures the issuer has established under the regulations.

### Duties of Users of Consumer Reports Regarding Address Discrepancies

The regulations impose new duties on consumer report users, including businesses that get consumer reports before deciding to extend credit. The regulations require them to respond appropriately when a consumer reporting agency informs the user of a substantial difference between the addresses the user reported to the consumer reporting agency and the address in the file for that consumer. When an address discrepancy report is received, the user must use reasonable policies and procedures to form a reasonable belief that the applicant and the consumer identified in the credit report are the same person. Reasonable policies and procedures may include comparing the information in the consumer report with information obtained in compliance with CIP regulations, information in the user's own records or information from a third party. Users also may verify the information in the consumer report with the consumer.

When a user has gotten a notice of address discrepancy from a consumer-reporting agency, the user must send the agency a consumer address the user has reasonably confirmed to be accurate. This obligation applies when the user (1) can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report; (2) has established a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy came.

### Detection, Prevention and Mitigation of Identity Theft

The heart of the regulations is the set of policies and procedures creditors and financial institutions must develop to help control identity theft. Those obligations include:

- Each must decide whether it offers or maintains covered accounts - a category that includes any account that permits multiple payments for the goods or services used for personal, family or household purposes. This review, which must be done periodically, includes an assessment of the methods the business provides to open accounts, access accounts, and its previous experiences with identify theft. If a determination is made that covered accounts are offered, it must implement a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with any new or existing covered account. The Program must include policies and procedures to respond appropriately to those Red Flags to prevent and mitigate identity theft.

- They also must update programs periodically to reflect changes in risks to customers and the safety and soundness of the business from identity theft. Initial Program approval must be obtained from the Board of Directors or an appropriate committee; the institution's staff must be trained to implement the Program; and the business must exercise appropriate and effective oversight of service provider arrangements.
- The specific Red Flags a Program will identify and address are not in the regulations. Covered entities must consider the suggestions made in a set of Interagency Guidelines on Identity Theft Defection, Prevention, and Mitigation. The Guidelines say each Program should include, as appropriate, Red Flags from the following categories:
  - **Alerts, notifications, or other warnings from consumer reporting agencies or service providers, like fraud detection services.** Red Flags in this category include a fraud alert or active duty alert included with a consumer report; a notice of credit freeze provided with a response to a consumer report; a notice of address discrepancy received from a consumer reporting agency; and information in the report that is inconsistent with the history and usual pattern of activity of an applicant or customer.
  - **The presentation of suspicious documents.** The Guidelines identify several categories including documents that appear to have been forged; photographs or physical descriptions that do not match the appearance of the person presenting the identification or other information on the identification that is not consistent with information provided by the customer or applicant; other information on the identification not consistent with readily accessible information on file with the business, like a signature card or a recent check; or an application that appears to have been altered or forged, or appears to have been destroyed or reassembled.
  - **The presentation of suspicious personal identifying information like a suspicious address change.** The Guidelines give a long list of examples of this category including an address that does not match any address in the consumer report; an unissued Social Security Number or one listed on the Social Security Administration's Death Master File; a lack of correlation between the items of information provided like a lack of correlation between the SSN range and date of birth; information associated with known fraudulent activity, like an address or telephone number previously provided on a fraudulent application; information commonly associated with fraud, like a mail drop or pager number; incomplete information; information inconsistent with personal information already on file with the business; and an inability to answer challenge questions.
  - **The unusual use of, or other suspicious activity related to, a covered account.** This can include a request for a new or replacement card shortly after a change of address; use of a new account in ways commonly associated with fraud, like purchasing jewelry or other items quickly convertible to cash; nonpayment on an account with no history of missed payments; a change in call patterns on a mobile phone account; use of a previously inactive account; return of mail to the customer as undeliverable; and a notice that the customer is not receiving paper account statements.
  - Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the

business. Examples include any notification that the business has opened a fraudulent account for a person engaged in identity theft.

### Records Security & Vendor Oversight

The regulations give businesses a great deal of discretion in identifying threats they must address and measures appropriate measures. Affected entities are required to take a number of factors into account, including: incidents of identity theft that the business has experienced; and any data security incident that results in unauthorized access to a customer's account records held by the business or a third party.

The implication is clear. A business that has experienced identity theft or a breach of data security that might or might not have resulted in identity theft will be expected to develop a program that adequately addresses the circumstances that gave rise to those incidents. It is also reasonable to expect a business that has experienced a data security or identity theft incident will be scrutinized much more closely when regulators investigate to ensure their identity theft prevention programs are rigorous and thorough.

Another important feature of the regulations is the obligation to exercise appropriate and effective oversight of service provider arrangements. As the agencies point out, a covered entity cannot escape its obligations to comply simply by outsourcing an activity. Instead, covered entities must exercise the degree of oversight appropriate in the circumstances. This requirement underscores the importance of careful vendor selection.

### **GETTING READY**

By May 1, 2009 all creditors and financial institutions subject to the regulations must have compliance programs in place. Because program development is a multi-step process and requires approval of the board of directors or equivalent level of management, the sooner affected organizations begin their program development, the better.

Among the steps that must be taken is confirmation the organization is subject to the regulations and maintains accounts of the kind a compliance program must cover. Generally speaking, any creditor or financial institution that provides or arranges for the provision of goods or services on credit should assume the Red Flags apply. Once the decision that Red Flags apply is made, the organization must conduct a risk assessment of all of the circumstances in its business operations that might present vulnerabilities for identity theft. This is also the time to identify past incidents of identity theft or data loss that the program must ensure against repetition of.