

The Red Flag Regulations: A New Front Opens in the War on Identity Theft

(UPDATED MAY 2009)

by Charles H. Kennedy, Of Counsel
Morrison and Foerster LLP

UPDATE: The Federal Trade Commission (FTC) announced on April 30, 2009 that it will delay enforcement of the Red Flag regulations a second time, until August 1, 2009. This white paper has been edited to reflect this new enforcement date.

The new “Red Flags” regulations are among the most important privacy initiatives of recent years. Creditors and financial institutions should begin now to develop programs that will put them in compliance with the new regulations on or before the deadline of August 1, 2009. This White Paper explains the regulations, their background and the compliance measures that affected organizations should be undertaking today.

On August 1, 2009, financial institutions and creditors in the United States will be required to comply with new “Red Flag” regulations adopted by the Federal Trade Commission (“FTC”) and the functional regulators of the nations’ financial institutions. The new regulations require each of those businesses to develop and implement programs designed to detect, prevent and mitigate the effects of identity theft.

This White Paper explores the problem of identity theft and the law’s responses to that problem, including the principal provisions of the Red Flag regulations. The Paper also offers some tips on how businesses can prepare themselves for the November 1 compliance deadline and avoid adverse actions from the regulators that are charged with enforcement of these regulations.

I. IDENTITY THEFT: WHY WE NEED THE RED FLAG REGULATIONS

Identity theft is the fraudulent use of an individual’s personal information to open financial accounts, incur debts or transact other business in the victim’s name. Identity theft also is a growth industry that imposes enormous financial and emotional costs on individuals and businesses alike.¹

In order to commit identity theft, a person must do two things: first, obtain another person’s personal information; second, successfully use that information to open an unauthorized account (“new account fraud”) or make unauthorized charges against an existing account (“existing account fraud”).²

Mr. Kennedy is Of Counsel in the Washington, DC office of Morrison & Foerster LLP. He is also an adjunct professor of law at the Columbus School of Law, Catholic University of America, and the author or co-author of four books on communications law. Mr. Kennedy can be reached at ckennedy@mofo.com.

¹ Identity theft was made a federal crime in 1998, with passage of the Identity Theft and Assumption Deterrence Act.

² A third and less common phenomenon, sometimes called “synthetic identity theft,” occurs when a thief “combines stolen information with fictional information to create a new, fake identity.” Stacey L. Schreft, “Risks of Identity Theft: Can the Market Protect the Payment System?”, *Economic Review (Kansas City)* (Federal Reserve Bank of Kansas City 2007).

In a case of existing account fraud, the thief first obtains those items of personal information that are needed to charge purchases against a victim's account, then uses those items to obtain goods or services that will be charged to the victim's credit card or other account. For example, the thief might acquire a victim's name, address and credit card number, then use that information to buy merchandise from an online retailer.

In the case of new account fraud, the deception is usually more complex. Before extending credit to a person who is not an existing customer or account holder, card issuers and other businesses want to confirm that the applicant is a good credit risk. Such a determination requires a substantial amount of information about the applicant's personal financial history – information that an impostor typically will not have.

Fortunately for the identity thieves, creditors typically do not ask the applicant to supply all of the information needed to assess the applicant's credit-worthiness. Instead, the creditors collect the applicants' detailed financial histories from third-party credit reporting agencies. To initiate this process, the creditor only needs to collect a few items of personal information from the applicant. When those items are submitted to the credit reporting agency, the agency will look for a file in its records that match those items and will furnish a copy of the complete file to the creditor. If the creditor is satisfied with the report, it typically will open a new account that permits the applicant (whether genuine or an impostor) to obtain goods or services on a deferred-payment basis. The thief acquires something of value and the victim gets the bills.

Prevention of identity theft and its effects, like the crime itself, is a multi-step process. The first and most effective step is to keep unauthorized persons from acquiring personal information in the first place. If that step fails, creditors and credit reporting agencies can prevent the successful misuse of the stolen data by requiring more information from new account applicants and persons seeking to make charges against existing accounts, or by taking steps to verify the identities of persons whose attempts to use or establish credit appear to be questionable. Finally, if all of those efforts fail and identity theft attempts are successful, businesses can soften the impact on consumers by forgiving unauthorized charges.

Creditors and financial institutions in the U.S. have made considerable efforts, even without legal compulsion, to make identity theft more difficult. Better records management and information security, especially in the financial services industry, have improved the security of stored personal information. Similarly, the Payment Card Industry Data Security Standard has imposed uniform data security measures on payment card processors and users. Existing account fraud has been made somewhat more difficult by payment cards that now include security codes, in addition to the account number, that only someone in possession of the card can provide. Also, payment card issuers have implemented sophisticated programs that spot suspect transactions and trigger notification to cardholders.

In addition to these voluntary efforts by U.S. businesses, the law has moved on at least five fronts to reduce the incidence and impact of identity theft.

First, a number of state, federal and foreign laws require organizations that maintain personal information to protect that information from unauthorized access, disclosure and use. These obligations, which include the Gramm Leach Bliley Act,³ the Fair Credit Reporting Act,⁴ the Disposal Rule of the Fair and Accurate Credit Transactions Act,⁵ the Health Insurance Portability and Accountability Act,⁶ and the secure records disposal laws now enacted by at least 28 states⁷ are intended to keep identity thieves from acquiring the personal information of others in the first place.

³ Gramm-Leach-Bliley Financial Modernization Act, Pub.L. No. 106 102, 113 Stat. 1338 (1999), codified at various sections of 12 United States Code and 15 United States Code.

⁴ 15 U.S.C. § 1681 *et seq.*

⁵ 16 C.F.R. § 682.3.

⁶ Pub.L. No. 104-191, 110 Stat. 1936 (1996).

⁷ See, e.g., Ariz. Rev. Stat. § 44-7601; A.C.A. § 4-110-104; Cal. Civ. Code § 1798.81; C.R.S. § 6-1-713(1); O.C.G.A. § 10-15-2; KRS § 365.725; MCL § 445.72; N.J. Stat. § 56-8-162; NY CLS Gen. Bus. § 399-h; N.C. Gen. Stat. § 75.64; Tenn. Code Ann. § 39-14-150(g); Tex. Bus. & Com. Code § 48.102; 9 V.S.A. § 2445; Rev. Code Wash. § 19.215.010; Wis. Stat. § 895.505.

A second front was opened in 2003, when California enacted the first data security breach notification law.⁸ Such laws, which now are in force in at least 43 states, are intended to give individuals notice when their personal data may have been compromised so that they can take action to minimize the risk or impact of identity theft.⁹

A third front in the legal war against identity theft is the enactment of so called “credit freeze” laws, which give consumers the right to block access to their credit reports by new creditors.¹⁰ These laws are intended to prevent identity thieves from successfully incurring debts or other obligations in consumers’ names.

The fourth recent initiative was the adoption, pursuant to the USA PATRIOT Act, of Customer Identification Program (“CIP”) regulations.¹¹ Those regulations require all banks, savings associations, credit unions and certain non-federally regulated banks to develop and implement procedures to verify the identity of each and every bank customer. When individual customers open new accounts, banks must at minimum obtain the individual’s name, date of birth, and address. Each bank’s program also must contain procedures for verifying the customer’s identity within a reasonable time after the account is opened, including verification through documents and non-documentary verification, such as contacting the customer or obtaining a report from a credit reporting agency.

These initiatives, important as they are, still leave a gap in the wall of legal protection against identity theft. Specifically, they do not necessarily identify all of the measures that creditors and financial institutions should take to spot and respond to questionable credit applications that are likely to be the work of identity thieves. The recent “Red Flag” regulations, intended to close this gap, impose new legal obligations on financial institutions and businesses of all kinds that extend credit to consumers. Specifically, not later than August 1, 2009, all such businesses must develop and have in place a program that identifies, and provides effective means for dealing with, suspicious circumstances that suggest a threat of identity theft to the businesses’ customers.

The Red Flag regulations are among the most important privacy initiatives in recent years. This White Paper sets out the principal Red Flags requirements and suggests how businesses can best use the months between now and the November 1 deadline to ensure their compliance with those regulations.

II. REQUIREMENTS OF THE RED FLAG REGULATIONS

A. The Regulations Affect a Wide Cross-Section of American Business

The Red Flags regulations were adopted as amendments to the Fair Credit Reporting Act. However, they have a broader impact than previous regulations adopted under the Fair Credit Reporting Act, which applies primarily to consumer reporting agencies. The new regulations must be observed by two very wide categories of businesses: “financial institutions” and “creditors.”

Financial institutions include any “State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.”¹²

⁸ Cal. Civ. Code § 1798.29(a).

⁹ See, e.g., A.C.A. § 4-110-105; Conn. Gen. Stat. § 36a-701; 6 Del. C. § 102(a); Fla. Stat. § 817.5681; O.C.G.A. § 10-1-912; HRS § 487N-2; 28 Idaho Code § 28-51-105; 815 ILCS 530/10(a); La. R.S. § 51:3074; Minn. Stat. § 13.055; Mont. Code Anno. § 30-14-704; N.J. Stat. § 56:8-163; NY CLS Gen. Bus. § 899-aa; N.C. Gen. Stat. § 75-65; N.D. Cent. Code § 51-30-02; ORC Ann. § 1347.12; R.I. Gen. Laws § 1-49.2; Tex. Bus. & Com. Code § 48.103(b); 9 V.S.A. § 2435(6); Rev. Code Wash. § 19.255.010; Wis. Stat. § 895.507

¹⁰ See, e.g., Cal. Civ. Code § 1785.10-1789.9.5; La. Rev. Stat. Ann. § 9:3571.1; Nev. Rev. Stat. § 598C.2-12; N.C. Gen. Stat. Ann. § 75-61; Conn. Gen. Stat. § 36a-701; N.J. Stat. Ann. § 56:11-46; N.Y. Gen. Bus. Law § 380-t.

¹¹ See 31 C.F.R. § 103.121.

¹² 15 U.S.C. § 1681a(t).

A creditor, in turn, is defined to include “lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.”¹³ Essentially, any person or entity that furnishes goods or services on a delayed-payment basis qualifies as a “creditor” for purposes of the Red Flag regulations.

B. Financial Institutions and Creditors Must Develop Compliance Programs

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. The following discusses each of these requirements in turn.

1. Duties of Card Issuers Regarding Changes of Address

Some of the Red Flag obligations are imposed specifically upon issuers of payment cards (i.e., debit cards and credit cards). Those entities must be prepared to deal with cases in which 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.¹⁴ In these cases, the card issuer may not issue an additional or replacement card until it has notified the cardholder of the request at the cardholder’s former address or by any 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 Red Flag regulations.

2. Duties of Users of Consumer Reports Regarding Address Discrepancies

The regulations also impose new duties upon users of consumer reports, including businesses that obtain consumer reports before deciding to extend credit. Specifically, the regulations require such users to respond appropriately when a consumer reporting agency informs the user of a “substantial difference” between the address the user reported to the consumer reporting agency and the address or addresses in the agency’s file for that consumer.¹⁵

When such an address discrepancy report is received, the user must employ reasonable policies and procedures to form a “reasonable belief” that the applicant and the consumer identified in the credit report are the same person.¹⁶ Reasonable policies and procedures may include comparing the information in the consumer report with information the user has obtained in compliance with the CIP regulations, information in the user’s own records or information obtained from a third party. Users also may verify the information in the consumer report with the consumer.

Also, when a user has received a notice of address discrepancy from a consumer reporting agency, the user must send to the agency a consumer address that 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 was obtained.

¹³ 16 C.F.R. § 681.2(5).

¹⁴ See, e.g., 16 C.F.R. § 681.3.

¹⁵ See, e.g., 16 C.F.R. § 681.1(c).

¹⁶ *Id.* § 681.1(c)(1).

3. Detection, Prevention and Mitigation of Identity Theft

The heart of the Red Flag regulations is the set of policies and procedures that creditors and financial institutions must develop in order to help control identity theft. Those obligations include several elements.

First, each creditor and financial institution must decide whether it offers or maintains covered accounts – a category that includes any account that permits multiple payments for the price of goods or services used for personal, family or household purposes.¹⁷ This review, which must be conducted periodically, includes an assessment of the methods the business provides to open accounts, the methods it provides to access the accounts, and its previous experiences with identify theft.¹⁸

If a financial institution or creditor determines that it offers covered accounts, it must develop and implement “a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.”¹⁹ The Program must include policies and procedures to identify “Red Flags” for the covered accounts, incorporate those Red Flags into the Program, detect Red Flags that have been incorporated into the Program, and respond appropriately to those Red Flags so as to prevent and mitigate identity theft.

Creditors and financial institutions also must update their programs periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft. Initial approval of the Program must be obtained from the Board of Directors or an appropriate committee thereof; the institution’s staff must be trained as necessary to implement the Program; and the financial institution or creditor must exercise “appropriate and effective oversight of service provider arrangements.”

The specific Red Flags that a creditor or financial institution’s program will identify and address are not set out in the regulations, but covered entities are required to consider the suggestions made in an accompanying set of “Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation” (“Guidelines”). The Guidelines are worth examining in detail.

Notably, the Guidelines state that each Program should include, as appropriate, Red Flags from the following categories:

- “Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.” Red Flags in this category include: (a) a fraud alert or active duty alert that is included with a consumer report; (b) a notice of credit freeze that is provided with a response to a consumer report; (c) a notice of address discrepancy received from a consumer reporting agency; and (d) 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 of suspicious documents, including: (a) documents that appear to have been forged; (b) photographs or physical descriptions that do not match the appearance of the applicant or customer presenting the identification; (c) other information on the identification that is not consistent with information

¹⁷ See 16 C.F.R. § 681.2(b)(3).

¹⁸ *Id.* § 681(c).

¹⁹ *Id.* § 681(d)(1).

provided by the customer or applicant; (d) other information on the identification that is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check; or (e) an application that appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

- “The presentation of suspicious personal identifying information, such as a suspicious address change.” The Guidelines give a long list of examples of suspicious personal identifying information, including: (a) an address that does not match any address in the consumer report; (b) a Social Security Number that has not been issued or is listed on the Social Security Administration’s Death Master File; (c) a lack of correlation between the items of information provided, such as a lack of correlation between the SSN range and date of birth; (d) information associated with known fraudulent activity, such as an address or telephone number previously provided on a fraudulent application; (e) information commonly associated with fraud, such as a mail drop or pager number; (f) incomplete information; (g) information that is inconsistent with personal information already on file with the financial institution or creditor; and (h) inability to answer “challenge questions.”
- “The unusual use of, or other suspicious activity related to, a covered account.” According to the Guidelines, this can include: (a) a request for a new or replacement payment card shortly after submission of a change of address; (b) use of a new account in ways commonly associated with fraud, such as purchase of jewelry or other items that are quickly convertible to cash; (c) nonpayment on an account with no history of missed payments; (d) a change in call patterns on a mobile phone account; (e) use of a previously inactive account; (f) return of mail to the customer as undeliverable; and (g) 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 financial institution or creditor.” Examples include any notification that the creditor of financial institution has opened a fraudulent account for a person engaged in identity theft.

4. The Importance of Records Security and Vendor Oversight

The Red Flags regulations give creditors and financial institutions a great deal of discretion in identifying the threats they must address and the preventive measures that are appropriate. Specifically, in identifying threats and developing measures for dealing with those threats, affected entities are required to take into account a number of factors, including: (1) incidents of identity theft that the financial institution or creditor has experienced; and (2) any data security incident that results in unauthorized access to a customer’s account records held by the financial institution, creditor, or third party.²⁰

The implication of these provisions is clear. A creditor or financial institution that has experienced identity theft, or even 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 that a creditor or financial institution that has experienced a data security or identity theft incident will be scrutinized much more closely, when regulators investigate those organizations, to ensure that their identity theft prevention programs are rigorous and thorough.

²⁰ 16 C.F.R. Part 681, Appendix A.

These elements of the regulations underscore the importance of addressing the fundamentals of data security, including protection of records containing personal information at all stages of the records' life cycle, including retention and disposal. Failure to secure sensitive records increases the likelihood of a compromise of personal information and close regulatory scrutiny of the organization's Red Flags program and all other aspects of the organization's privacy compliance.

Another important feature of the Red Flags regulations is the obligation to "[e]xercise appropriate and effective oversight of service provider arrangements."²¹ As the agencies that adopted the Red Flag regulations point out, "a covered entity cannot escape its obligations to comply with the final and to include in its Program those guidelines that are appropriate simply by outsourcing an activity."²² Instead, covered entities must exercise the degree of oversight that is appropriate in the circumstances. This requirement underscores the importance of careful vendor selection.

III. GETTING READY FOR THE RED FLAG REGULATIONS

By August 1, 2009, all creditors and financial institutions subject to the Red Flag regulations must have their compliance programs in place. Because development of such a program is a multi-step process and requires approval of the organization's 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 that the organization is subject to the Red Flags regulations and maintains accounts of the kind a Red Flags compliance program must cover. Generally speaking, any creditor or financial institution that provides or arranges for the provision of goods or services on a deferred-payment basis should assume that the Red Flags apply.

Once the decision that the Red Flags apply is made, the organization must conduct a careful 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.

When the program is put in place and implementation has begun, organizations must keep in mind that the program is only as good as the training, oversight and periodic modifications that will keep it relevant and effective. Above all, avoidance of data loss and identity theft incidents is the surest way to prevent regulatory action, lawsuits and other fallout that can harm your organization's financial viability and reputation.

²¹ 16 C.F.R. § 681.2(e)(4). Affected institutions also must train staff to implement the Program and update the Program as necessary. Id. § 681.2(d)(2)(iv), (e)(3).

²² 72 FR 63718, 63732 (Nov. 9, 2007).

©2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

 **IRON MOUNTAIN®**
745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout North America, Europe, Latin America, and Asia Pacific.

For more information, visit our Web site at www.ironmountain.com.