CNA

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Red Flags Rule Does Not Apply to Lawyers…For Now

NEW RED FLAGS LEGISLATION:

On December 18, 2010, President Obama signed into law the Red Flag Program Clarification Act of 2010 ("Clarification Act")[1] that exempts lawyers from rules promulgated by the Federal Trade Commission ("FTC") requiring businesses to implement a written *Identity Theft Prevention Program* designed to detect the warning signs (a.k.a "Red Flags") of identity theft in their daily operations.

The Clarification Act establishes that lawyers as well as other professional service providers should not be generally classified as "creditors" for the purposes of the Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").[2, 3, 4] There had previously been some dispute over whether lawyers should be considered "creditors" under the broad definition, as interpreted by the FTC, to the extent that lawyers sometimes allow clients in the course of their representation to pay for professional services after the services are performed (e.g., monthly billing).

In addressing the current legislation, the Clarification Act states, in part, that the term "creditor" refers only to a business that regularly and in the ordinary course of business:

(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

(ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

(iii) advances funds to or on behalf of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.[5]

The Clarification Act specifies that it does not include funds advanced on behalf of a person "for expenses incidental to a service provided by the creditor to that person."[6]

BRIEF HISTORY OF RED FLAGS LEGISLATION:

On November 9, 2007, in response to FACT Act, the FTC issued the Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule ("Red Flags Rule").[7] The Red Flags Rule provided categories and illustrative examples of Red Flags that may be used by creditors in implementing their Red Flags Policies. However, there was still confusion as to who was a creditor and would therefore be required to comply with the Red Flags Rule.

In April 2009, after various professional organizations, including the American Bar Association ("ABA"), sought clarification of the term "creditor", the FTC issued its Extended Enforcement Policy: Identity Theft Red Flags Rule ("Policy").[8] The Policy specified that, "[t]his rule applies to all entities that regularly permit deferred payments for goods or services, including entities such as health care providers, attorneys, and other professionals, as well as retailers and a wide range of businesses that invoice their customers."[9]

1 See Bill Text Versions, 111th Congress (2009-2010) S.3987 Red Flag Program Clarification Act of 2010 at **http://www.gpo.gov/fdsys/pkg/BILLS-111s3987enr/pdf/BILLS-111s3987enr.pdf**

2 Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. § 1681 *et seq.* at **http://www.ftc.gov/os/statutes/fcradoc.pdf**

3 Fair and Accurate Credit Transactions Act of 2003 (FACT Act), Pub. L. No. 108-159, at **http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf**

4 In the "Colloquy in Support of Legislation Clarifying the Definition of Creditor under the FTC 'Red Flags' Rule," Senator Dodd, as Chairman of the Senate Banking Committee, indicated that the "legislation also makes clear that lawyers, doctors, dentists, orthodontists, pharmacists, veterinarians, accountants, nurse practitioners, social workers, other types of health care providers and other service providers will no longer be classified as 'creditors' for the purposes of the Red Flags Rule just because they do not receive payment in full from their clients at the time they provide their services, when they don't offer or maintain accounts that pose a reasonably foreseeable risk of identity theft." See **http://www.abajournal.com/files/FTCRedFlagsColloquyFINAL.pdf**.

5 See Note 1 infra.

6 Id.

7 The Red Flags Rule, at **http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf**

8 FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.1, at **http://www.ftc.gov/os/2010/05/100528redflagsrule.pdf**

9 Id.

In response to the Policy, the ABA filed suit in federal district court against the FTC alleging that the FTC was acting beyond the powers granted to it under the FACT Act.[10] The district court granted summary judgment in favor of the ABA and found that "…the Red Flags Rule cannot be properly applied to attorneys."[11] The FTC appealed the district court's findings. Since during the course of the appeal, the Clarification Act was signed into law, the appellate court subsequently dismissed the entire ABA action as moot.[12]

The appellate court specified that its dismissal ruling was based upon the recent legislative action. The court noted that the FTC might in the future attempt to institute "*new* rules" or "*new* enforcement policies" to regulate lawyers and law firms, but that it would not make any decisions concerning "merely hypothetical possibilities."[13] It is not known what the FTC intends, if anything, to do in the future with regard to imposing rules such as the Red Flags Rule on attorneys and other professionals.

MANAGING IDENTITY THEFT RISKS EVEN WITHOUT RED FLAGS RULE:

While for now lawyers will not be required by law to implement a written identity theft program in their practices, from a risk control perspective, it is prudent for lawyers to remain vigilant in preventing identify theft. In their daily practice, lawyers should attempt to identify any pattern, practice or specific activity that indicates the possible existence of identity theft.

In particular, lawyers should look for activities indicating the possible existence of identity theft that fall into five specific categories as provided by the FTC in the Red Flags Rule:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information, such as a suspicious address change;
4. The unusual use of, or other suspicious activity related to, a covered account; and
5. Notice from customers, victims of identify theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.[14]

If lawyers suspect identity theft may be occurring, they should consult with external experts as needed to investigate and respond quickly to help prevent and mitigate any further damage. Proper response may include monitoring accounts for additional evidence of identity theft, contacting the client, asking for additional identifying information, calling law enforcement and changing any security device that permits account access.[15]

If the investigation indicates that a privacy breach may have occurred, the lawyers should consult with their insurance agent or broker regarding applicable insurance coverage and reporting obligations under their policies. They should promptly research their obligations under state and federal privacy and security laws to notify and provide remediation services (such as credit monitoring) to clients and third parties that may have had personally identifiable information exposed to unauthorized parties.[16] Finally, they should consult with experts in privacy and security to determine if additional controls should be instituted to prevent future privacy breaches.

The FTC has published a "do it yourself" template to establish an identity theft prevention program for businesses available as a free download, which lawyers and their clients may find helpful.[17]

GENERAL AWARENESS OF INDUSTRY AND PROFESSION-SPECIFIC PRIVACY AND SECURITY RULES:

Lawyers should also be aware of other privacy-related laws, regulations and rules that apply to specific industries and professions. For example:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy rule applies to health care providers, health plans and health care clearinghouses and governs the handling of individually identifiable health information. HIPAA also can apply to advisors to those institutions, including lawyers, depending upon the circumstances.
- The Gramm-Leach-Bliley Financial Modernization Act of 1999 ("GLB Act") resulted in the issuance of the Privacy and Safeguards Rules by the FTC, which apply not only to traditional financial institutions such as banks and savings and loan associations, but also to non-bank industries such as mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. If the law firm

10 American Bar Association v. Federal Trade Commission, Civil Action No. 09-1636, at **http://www.americanbar.org/content/dam/aba/migrated/media/nosearch/1_1_Complaint.authcheckdam.pdf**
11 ABA v. FTC Memorandum Opinion, December 1, 2009, at **http://www.americanbar.org/content/dam/aba/migrated/poladv/priorities/redflagrule/2009dec01_memoropinion.authcheckdam.pdf**
12 American Bar Association v. Federal Trade Commission, No. 10-5057 (D.C. 2011), at **http://www.ftc.gov/os/2011/03/110304americanbarassociation.pdf**
13 Id.
14 Please see attached Appendix A for the complete text of categories of Red Flags and illustrative examples as provided by the FTC in the Red Flags Rule.
15 See Kobus, Theodore J. and Silvestri, Mark, "Red Flags Rule Raise Stakes on Identity Theft Prevention" June 2010.
16 Listings of state security breach notification laws are maintained by the American Institute of Certified Public Accountants and the National Conference of State Legislatures on their websites at **http://www.aicpa.org** and **http://www.ncsl.org**
17 **http://www.ftc.gov/bcp/edu/microsites/redflagsrule/diy-template.shtm**

represents such industries, these rules should be reviewed, and systems for compliance should be implemented.

- Lawyers must also comply with professional ethics rules and regulations applicable to the handling of confidential client information.[18]

SUMMARY:

While the Red Flags Rule does not currently apply specifically to lawyers, the constantly changing landscape of laws, regulations and rules concerning privacy underscores the importance of a coordinated approach to risk control. The trend is clearly toward laws that require pro-active safeguards and some may be broadly applicable to all industries.

Lawyers should consider designating an individual within their firm who is responsible for instituting and monitoring appropriate controls to ensure compliance with all current and future privacy and data security requirements. It will continue to be critical for lawyers to identify the risks associated with identity theft and other privacy-related violations, and to be prepared to manage those risks.

18 See Id.