

Lawyers required to protect personal information under new federal rule

By Susan D. Oja and Alex De Grand

April 1, 2009 -- Lawyers who bill their clients after services have been rendered are expected to implement a written program guarding against the theft of their employees' and clients' personal information under a new federal law./p>

The Federal Trade Commission will begin enforcement of the "red flags rule" on May 1. The rule is part of the **Fair and Accurate Credit Transactions Act** of 2003 (FACTA), a congressional response to **spikes** in reported identity theft. Identity thieves assume a person's entire identity or synthesize one from parts of various victims. **Because more than half of identity thefts occur in the workplace, businesses are required to implement safeguards.**

Those subject to the rule are "creditors" and financial institutions who maintain consumer-type accounts or other accounts at reasonable risk of identity theft. The FTC noted that identity thieves look for opportunities to obtain products or services that do not require payment up-front.



As interpreted by the FTC, "creditors" has a broad definition, encompassing professionals such as lawyers and doctors who defer payment of a client's bill. The American Medical Association protested that other federal laws and professional ethical duties to maintain patient confidentiality precluded the new rule. But the FTC held in a **letter** that the statute borrows the sweeping definition of "creditor" from the Equal Credit Opportunity Act (ECOA). Agency **interpretation** of the ECOA specifically includes doctors and lawyers within the meaning of "creditor."

What is expected

Under the new rule, lawyers must implement a written policy specifying how they will watch for the warning signs -- the "red flags" -- that indicate an identity theft may be occurring and how they will respond to prevent or mitigate the crime if uncovered.

Policies are supposed to be tailored to the amount of risk. The FTC acknowledges there is no bright-line rule to distinguish between high and low-risk. But the rule suggests a lawyer consider such factors as how easily an account is opened or accessed and previous experience with identity theft.

If a lawyer finds there is little risk, an appropriate program might comprise no more than checking photo id at the time services are sought and a policy against collecting from an identity theft victim or reporting it on the victim's credit report.

In its letter to the AMA, the FTC stated that it does not foresee the new rule imposing a great burden. "For example, a small medical practice with a well-known, limited patient base might have a lower risk of identity theft, and thus might adopt a more limited Program than a clinic in a large metropolitan setting that sees a high volume of patients," the letter read.

What to watch for

The **Appendix** of the "red flags rule" provides examples of incidents putting a creditor lawyer on notice of potential identity theft. In addition to fraud alerts from consumer credit agencies or the client's complaint, this list includes suspicious documents, perhaps altered or forged. A creditor lawyer may receive fishy personal information such as an unexpected change of address. Creditor lawyers are also directed to look for unusual use of an account.

A creditor lawyer's policy should address the detection of "red flags" at the time an account is opened by obtaining identifying information about the new client and verifying it, the rule instructs.

What to do

Responses to “red flags” should be in proportion to the risk posed and a creditor lawyer is advised to consider any “aggravating factors” such as a data security breach that may exacerbate the threat. The rule Appendix suggests appropriate responses could be alerting law enforcement, monitoring the account for evidence of identity theft, changing passwords or other security devices controlling account access, reopening an account with a new account number, or closing an account. Under certain circumstances, the rule states that a creditor lawyer may determine no response is necessary.

These written policies should be updated periodically to account for changes in risks to clients’ information or innovations in detection of identity theft. A subsequent merger, acquisition, joint venture, or service provider arrangement may also prompt the need for an updated written policy.

The rule also requires appointing a senior management person to implement the program; appropriately educating employees; and overseeing any service provider arrangements. Liability follows a creditor lawyer’s data, so due diligence is necessary to confirm vendor compliance before outsourcing payroll or hiring an office cleaning company.

More information from the FTC: **[The Red Flags Rules: Are you complying with new requirements for fighting identity theft?](#)**

Susan D. Oja, a solo practitioner in Middleton, is a certified identity theft risk management specialist through the Institute of Fraud Risk Management. Alex De Grand is a legal writer for the State Bar of Wisconsin.

<http://www.wisbar.org/AM/Template.cfm?Section=InsideTrack&Template=/CustomSource/InsideTrack/contentDisplay.cfm&ContentID=79574>