IDENTITY THEFT: PROTECT YOURSELF AND YOUR CLIENTS

By Mari J. Frank

Mari J. Frank

Massive security breaches of sensitive personal information are on the rise, and identity theft continues to claim million of victims. It could happen to you, your firm, or your clients.

When a woman I never met, in a city four hours north of my office, stole my own identity, I was shaken. In 1996, my "evil twin" stole over $50,000 worth of credit in my name, and worse yet assumed my profession as an attorney distributing business cards with my name. At that time there were no laws making identity theft a crime at the state or federal level (for consumer victims). Since then, I have participated in task forces, helped write legislation, and testified before Congress and the White House as an advocate for other victims.

You certainly have seen horror stories about this crime on television, and you may be concerned about this happening to you, your firm, your family, or your clients—since no one is immune. A 2010 report by Javelin Strategy & Research found that the instances of identity theft reached record numbers in 2009, with an estimated 11.1 million adult victims, and a total amount of $54 billion in fraud.

Americans are worried about identity theft. According to an October 2009 Gallup Poll, 66 percent of respondents said they frequently worried about identity theft. *See* www.gallup.com. My goal in this article is to help you understand your vulnerabilities, and to give you tools to minimize both your personal and professional risk.

The truth is, no matter how careful you are with your information, you, your firm and your clients are vulnerable because sensitive information is out of your control when it is in the hands of third party companies, government agencies, or hackers. The crime of identity theft has skyrocketed due to careless information handling practices by businesses, organizations and government entities that collect, store, utilize, and share your personally identifiable data. Without strict guidelines and real enforcement (allowing a private right of action), the problem has grown worse.

As an attorney, you have an affirmative duty to protect the sensitive records of your staff and clients. Most states, including California, have security breach notification laws. *See, e.g.*, Cal. Civil Code sections 1798.29, 1798.82, and 1798.84, which require all businesses and state governmental agencies that experience a security breach (an acquisition of unencrypted electronic files of sensitive information by unauthorized persons,) to notify all potential victims of the breach so that they may protect themselves with a fraud alert, a security freeze or other means.

Federal guidelines for financial institutions encourage safeguards and notification, as well as the Gramm-Leach Bliley Act (15 U.S.C §§6801 – 6809). On August 19, 2009, the federal Department of Health and Human Services (HHS) issued the interim final rule regarding notification of breaches of unsecured protected health information under the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164). There are numerous pending federal bills that would require alternative security breach triggers for notification, and would preempt state laws. Over a five year period, from February 15, 2005 through November 15, 2010, there was public reporting of the security breach of 511,637,407 records of personal identifying information. (For an update of current breaches please visit http://www.privacyrights.org/ar/ChronDataBreaches.htm.) It's important to

continued on page 15

remember that not all security breaches must be publicly reported, and of those that are reported, many of the incidents don't reveal the actual number of records lost or stolen.

Before you can protect yourself, your staff, your firm and your clients from identity theft, you must understand just exactly what it is and how it happens. Simply, you become a victim of identity theft when an unauthorized person uses your personal identifiers, like your name, your Social Security Number ("SSN"), or other unique identifiers, to impersonate you and to commit fraud. Individuals, businesses and law firms may all become victims. Imposters will steal identities for four main reasons: financial gain (the major reason), to avoid arrest or prosecution, revenge, jealousy, and terrorism. There is no limit to the creativity of these impostors, because whatever you can do or obtain with your identity (personal or business), your impersonator can also do as your "clone."

Using your credit is an easy way for criminally minded persons to steal from innocent, good people like you. With this "faceless crime," a perpetrator doesn't have to use a gun or ever meet the victim. All he or she needs is a bit of information. Right now the key to the kingdom of identity theft is the SSN. In the near future it may be a fingerprint, an iris scan, or other unique "piece of your body" called biometric information that is transferred electronically via the Internet; it may even be a radio frequency identifier (RFID). No matter the method, the game is the same: fraud.

Not only can thieves obtain new credit and credit cards using your information, but they can also siphon money from your bank accounts, investment accounts, trust funds, college accounts, and retirement plans. They can obtain life insurance using a victim's name (and make themselves the beneficiary), secure medical services, have babies using an identity fraud victim's health insurance, obtain medical care, steal disability payments or Social Security checks, receive unemployment or disability compensation, obtain a victim's tax refund, and even file bankruptcy using a victim's identity. They can create bank accounts in your firm's name and deposit fraudulent checks, and your firm is later on the hook.

Consider all the places that have your SSN and other personal identifying information, including your CPA, the IRS, the State Tax Board, credit bureaus, your creditors, your bank, investment institutions, your law firm, etc.—the number is daunting. Without the ability to control access, there is no guarantee, no matter how careful you are, that you won't become a victim yourself. In your law firm you can control how information is collected, viewed by others, stored, secured and protected. You have a duty to safeguard information that is within your control.

The Red Flag Rules Intended to Prevent Identity Theft May Apply to Lawyers

A few years ago, the American Bar Association filed a complaint against the Federal Trade Commission ("FTC") alleging that the Commission's application of The Identity Theft Red Flag Rule under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007) to attorneys exceeds the Commission's statutory authority. On October 29, 2009, District Judge Reggie Walton of the District of Columbia agreed, holding that Congress did not intend lawyers to be considered "creditors" under the Act. Under Walton's decision, the Red Flag Rule is inapplicable to lawyers outside the financial sector.

However, on February 25, 2010, the FTC filed an appeal of the judge's decision. On November 15, 2010, the U.S. Court of Appeals for the D.C. Circuit heard oral argument regarding whether the FTC has the authority to regulate the legal profession. The ruling in this case is important because it could require law firms big and small to implement anti-fraud measures and would expand federal power to regulate lawyers, which many believe should be left to the states.

Whether or not the Court rules that law firms are subject to the Red Flag Rule, lawyers have an affirmative duty to protect clients and staff from identity theft. Indeed, if any of our clients or employees becomes victims of identity theft due to our failure to take reasonable steps to protect their sensitive data from fraudsters, we may be subject to liability. Although the FTC (and other government agencies) may not bring an enforcement action against you or your firm based on the Red Flag Rules, it's nevertheless a good idea to implement the rules because as "reasonable measures" they will help shield you from liability if the worst happens.

The Red Flag Rules provide guidance on how to develop, implement, and administer identity theft

continued on page 16

prevention programs. Such programs must include four basic elements, which together create a framework to address the threat of identity theft as follows:

1. The program must include reasonable procedures to identify the "red flags." For example, if a client has to provide some form of identification to retain your firm, a driver's license that looks like a fake would be a "red flag."
2. Your policies must be designed to detect the red flags you've identified. For example, if you've identified fake IDs as a red flag, you must have procedures in place to detect possible fake, forged, or altered identification.
3. Your policies must clarify what actions you'll take when you detect red flags. If you believe that a staff member has accessed a file without authority, who will be notified?
4. You must address how you will re-evaluate your policies periodically to reflect new risks and you must update and train your staff as to the risks and how to respond. You should log possible privacy and security breaches and address how to prevent them.
5. You must designate a senior level lawyer to approve your written program and policies. Your written program must state who is responsible for implementing, administering, training and enforcing the policies.

The following will assist you in creating an effective theft protection program.

Consider these general tips:

- Don't collect sensitive data you don't need and protect what you must store.
- Keep your sensitive records under lock and key
- Limit access to those who need to know, and monitor audit trails.
- Shred confidential data. Federal law requires complete destruction of personal information under the Fair Credit Reporting Act (FCRA §628; 15 U.S.C. §1681). This disposal rule applies to attorneys.
- Secure faxes, printers, computers, and emails.
- Conduct civil and criminal background checks for all employees and vendors with access to sensitive information about staff and clients.
- Limit use of SSN for client's and staff. Under California Civil Code §1798.85, companies may not do any of the following: 1) Post or publicly display SSNs; 2) Print SSNs on identification cards or badges; 3) Require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted; 4) Require people to log onto a Web site using an SSN without a password; or 5) Print SSNs on anything mailed to a client unless required by law or if the document is a form or application.
- Never include the SSN or sensitive financial data in public court records.
- Use photo business cards, photo ID's and photo credit cards to authenticate your office
- Authenticate who your clients are as well as your staff.

Secure Your Handhelds

- Encrypt confidential information.
- If you are transmitting wirelessly, then ensure proper user/device authentication before transmission.
- To protect data in case the device is lost or stolen, utilize user ID and password level security, and encrypt sensitive data.
- To find out more on how to protect yourself with wireless devices, visit the Web at www.firewallguide.com/index.htm.

Protect Your Office Computer

- Set up unique system passwords to access your computer.
- Install hardware and software firewalls and make sure staff use them and update software.
- Install, use, and continually update anti-virus and antispyware software. Run live updates.
- Set up automatic updates for all programs, and download in a timely manner.
- Back up your files daily and encrypt sensitive confidential files.
- Don't share or transmit data about clients without their permission and always encrypt with a password—teach your clients to do the same.
- Set forth privacy policies with regard to the use of the Intranet and taking files home—either in hard copy or electronically.

continued on page 17

Protect Your Office on the Internet

- Monitor social networking and blogging sites.
- Adopt office policies and procedures and make sure they are followed.
- Be cautious with peer-to-peer file sharing at home and the office.
- Don't trust clients and associates you meet online; use a nickname for your screen name.
- Make sure you are on the correct Web site of the company that you are doing business with, and not an imposter. Online fraudsters create Web site names (URLs) very similar to those of legitimate companies (this is called "Pharming"). To check whether the site that you're on is really the legitimate company, go to www.whois.net.
- Only give out information that is necessary for a specific transaction.
- Use disposable forwarding email addresses for chat rooms, purchases, public postings, and social networking.
- Never use a public computer, such as an Internet café, a library, or airport computer to access your sensitive information.
- Teach your clients not to send sensitive data by email. WinZip is an easy to use free program and you can teach your clients.
- Search out your name, your clients' and staff members' names on the Web to find what information is circulating.
- Don't get hooked by a "phishing" or " "vishing" expedition. Never respond to email or voicemail asking for sensitive information.
- Advise staff and clients not to put confidential or controversial information in email, in blogs, or on Web sites.
- Visit an Internet safety organization such as Cyber Angels to protect your identity (www.cyberangels.org) or the FTC (www.FTC.gov), for additional precautions.
- Designate a staff member to be in charge of Privacy and Identity theft protections.
- Implement Privacy and Identity Theft Policies on the Web and in your brochures. The Online Privacy Protection Act of 2003—California Business and Professions Code §§22575-22579 requires operators of commercial Web sites or online services that collect personal information on California residents through a Web site to conspicuously post and comply with its privacy policy.
- Train your staff on best practices for privacy and identity theft protection (visit www.identitytheft.org; www.privacyrights.org; www.ftc.gov; and www.idtheftcenter.org).
- Keep abreast of current privacy and identity theft laws. (Visit www.FTC.gov and the California Office of Privacy Protection for updated laws at www.privacy.ca.gov).

As a lawyer, you must collect and utilize confidential information about your clients and your employees. You have a duty to guard your clients' and staff's privacy and identity in your office and in court. This daunting challenge presents legal questions, security risks, and litigation exposure. Take the opportunity to analyze and enhance your information management practices, and create a proactive approach to data privacy and security. By implementing a privacy audit you will boost your clients' trust and goodwill, and increase profits. Implement the suggestions in this article to augment your privacy environment to protect your firm and safeguard your clients and your staff.

Mari J. Frank, *Esq., CIPP is the author of* The Identity Theft Survival Kit, Safeguard Your Identity, *and* The Complete Idiot Guide To Recovering From Identity Theft. *Since 2005 Mari has hosted Privacy Piracy, a weekly public affairs radio show dedicated to privacy issues airing at KUCI 88.9 FM and www.kuci.org/privacypiracy. She has testified on privacy issues in courts nationally, in the California legislature, the U.S. Congress and at the White House on Consumer Privacy on C-SPAN TV. Mari hosted a 90 minute PBS Television special, "Identity Theft: Protecting Yourself in the Information Age." She's an advisor to the State of California Office of Privacy Protection, a Privacy Fellow with the Ponemon Institute, a certified MCLE trainer and currently teaches at the University of California, Irvine. She's appeared on Dateline, 48 Hours, the O'Reilly Factor, Investigative Reports, NBC and ABC Nightly News, CNN, Geraldo, CNBC, Montel, Fox 11, 350 radio shows and has been featured in the ABA Journal, The California Bar Journal, The Wall Street Journal, USA Today, The Chicago Tribune, The LA Times, and The New York Times. Ms. Frank may be contacted at (949) 364-1511 and via email at Mari@MariFrank.com. See also www.identitytheft.org; www.kuci.org/privacypiracy; and www.MariFrank.com.*