IN BRIEF

THIS ISSUE
August 2008
Issue 105

Oregon State Bar
PROFESSIONAL LIABILITY FUND
www.osbplf.org
Malpractice Prevention Education for Oregon Lawyers

Protect Client Information From Identity Theft

Did you know that in 2006 Oregon ranked as the 13th worst state for identity theft in number of victims per capita? According to the Federal Trade Commission, this crime costs U.S. businesses nearly $48 billion every year. As keepers of confidential client information, lawyers are particularly vulnerable.

The Oregon Consumer Identity Theft Protection Act (the Act) passed by the 2007 legislature (ORS 646A.600 to 646A.628) gives businesses some guidance in the protection of sensitive information that is collected, kept, and shared. The law contains three main components that will help protect sensitive information: (1) protection of Social Security numbers; (2) general safeguards for data; and (3) notification of a security breach. The safeguard standards became effective January 1, 2008; the remainder of the law became effective October 1, 2007.

Some law firms will not need to make any additional changes to their law practice to comply with the Act. In fact, many firms have already implemented most of the requirements because of the inherently confidential nature of operating a law practice.

Does the Act Apply to Lawyers?

The new law applies to lawyers who, in the course of their practice, maintain or possess an individual's personal information. "Personal information" means an individual's unencrypted or unredacted first name or first initial and last name in combination with any one or more of the following:

(1) Social Security number;

(2) Driver license number or state identification card;

(3) Passport number or other U.S.-issued identification card;

(4) Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account.

Many law firms already comply with the Act because of the requirements of the Oregon Rules of Professional Conduct. Under ORPC 1.15-1, "Safekeeping Property," a lawyer has a duty to appropriately safeguard a client's property. A client file is considered client property; thus the information contained in a client file must be appropriately protected. *See* Oregon Formal Ethics Opinion No. 2005-125, fn 2. ORPC 1.6 requires lawyers to keep confidential any "information relating to the representation of a client." In addition, the Act does not apply to law firms who comply with state or federal law that provides greater protection to personal information, such as Title V (the privacy provisions) of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR parts 160 and 164).

What Does the Act Require?

The focus of the Act is to provide businesses with reasonable safeguards and procedures in handling and disposing of personal information and to protect the security, confidentiality, and integrity of the information.

One requirement that may be new to lawyers is that Social Security numbers must be redacted

Continued on page 2

on any materials that are mailed, publicly posted, or publicly displayed. This requirement does not apply to the use of SSNs for internal verification purposes or as required by state or federal law. Counties around the state have made available a UTCR Form 2.100 Affidavit that segregates personal information from documents that are filed in court. The requirement does not apply to judgments, court orders, or indictments filed before October 1, 2007.

If you collect any personal information, consider confirming in your fee agreement or engagement letter that the information will be used only to provide legal representation to the client. If your client's case necessitates mailing documents that include Social Security numbers, you might also want to get the client's written consent.

For law practices that do not currently have a security program in place, these are the minimum requirements that should be implemented to comply with the Act:

- **Administrative safeguards** – Identify what information the firm collects, where it is stored, and how to keep it safe; train employees in the security program; ensure that contracted service providers will protect personal information.

- **Technical safeguards** – Assess risks in your computer network and software programs; put in place safeguards to detect, prevent, and respond to attacks or system failures; test the safeguards to make sure they work.

- **Physical safeguards** – Protect against unauthorized access to or use of personal information.

The compliance standard for businesses with 50 or fewer employees is to have safeguards and disposal measures that are "appropriate to the size and complexity of the small business, the nature and scope of its activity, and the sensitivity of the personal information collected."

Practitioners must dispose of personal information by burning, pulverizing, shredding, or erasing electronic media. When recycling an old computer, the hard drive must be cleaned, destroyed, or reformatted. For information on file management, retention, and destruction, go to **www.osbplf.org.** Under Loss Prevention, select Practice Aids and Forms, then select File Management.

Your security program should also include securely storing sensitive information by using passwords and encryption and by securing information on portable devices such as laptops, USB Flash Drives, and PDAs. (*See* "Easy to Use or Easy to Lose? How to Protect Mobile Devices," page 7.)

What to Do After a Security Breach

The good news is that the Act gives law firms guidance on how to notify clients of a security breach. A "breach of security" is an "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information." A breach of security can occur when a laptop or portable device is lost or stolen, or any time a computer hacker or an unauthorized person accesses personal information of a client.

If you discover that a security breach has occurred, you must immediately notify those individuals whose information has been breached. You can notify clients by (1) mail; (2) e-mail (if this is the usual way you communicate with your client); (3) telephone; or (4) substitute notice, in limited circumstances, involving large cost or volume, as specified by the Act. Whichever method of notification you select, be sure to document your efforts.

The notice must include the following information:

(1) a general description of the security breach;

(2) the approximate date the breach occurred;

(3) the type of personal information obtained as a result of the breach;

(4) your firm's contact information;

(5) contact information for national consumer reporting agencies; and

(6) advice to the individual to report suspected identity theft to law enforcement, including the Federal Trade Commission.

For a sample notification letter, go to **www.osbplf.org**. Under Loss Prevention, select Practice Aids and Forms, then select Client Relations.

Notification is not required if, after an investigation or after consultation with law enforcement agencies, you determine that there is no reasonable likelihood of harm to the client whose personal information has been breached. When making this assessment, consider ORPC 1.4(b), which requires lawyers to explain matters to cllients to the extent necessary for them to make informed decisions. Also, if your judgment about whether to make the disclosure is impacted – because you or someone in your firm was responsible for the breach – you may have a conflict due to a personal interest under ORPC 1.7(a)(2). You must document your determination in writing and retain it for five years.

If you discover a breach of security affecting more than 1,000 clients, you must immediately report your notification steps to all national consumer reporting agencies. Currently,

there are four: Equifax, TransUnion, Experian, and Innovis. Your report should include the timing, distribution, and content of the notification given and the police report number, if available.

Post–security breach services, such as ID TheftSmart (**www.idtheftsmart.com**), offer identity restoration and credit monitoring services.

A PLF practice management advisor is available to meet with you to discuss your firm's security plan and suggest other safeguards you may want to implement. You can reach Beverly Michaelis at 503-924-4178 or beverlym@osbplf.org; Sheila Blackford at 503-684-7421 or sheilab@osbplf.org; and Dee Crocker at 503-924-4167 or deec@osbplf.org.

Kimi Nam
PLF Staff Attorney

Thanks to Helen Hierschbiel, OSB Deputy General Counsel, for her assistance with this article.

Identity Theft Protection
PLF/OSB Resources

Disaster Recovery

- Managing Practice Interruptions
- Protecting Your Firm (includes Web resources)

Technology

- How to Back Up Your Computer
- Application Service Providers

File Management

- File Retention and Destruction

Client Relations

- Notice to Clients re Theft of Computer Equipment

***In Brief* Articles:**

- Act Now to Avoid Disaster (May 2008)
- GLB Privacy Notice (Tips, Traps, & Resources, February 2006)
- Document Destruction (June 2005)
- Do You Need to Know about HIPAA? (June 2003)

***Oregon State Bar Bulletin* Articles:**

- The Lawyer's Guide to Mobile Computer Security (November 2007)
- Metadata: Guarding Against the Disclosure of Embedded Information (April 2007)
- Metadata: Danger or Delight? (May 2006)

Additional Resources

State of Oregon's Division of Finance and Corporate Securities (DFCS): http://www.cbs.state.or.us/dfcs/id_theft.html. Contains sample notification letters, tips for protecting data, contact information for DFCS representatives who can present information to your firm, and other resources.

Credit Reports and Credit Reporting Agencies: Consumers can obtain a free credit report once every 12 months. Free Annual Credit Report **www.annualcreditreport.com** will link you to three of the four national credit reporting agencies (Equifax **www.equifax.com**; Experian **www.experian.com**; TransUnion **www.transunion.com**). Innovis is the fourth (**www.innovis.com**).

Federal Trade Commission: www.ftc.gov/infosecurity. Provides information for businesses about keeping information secure. Includes a tutorial and related articles on protecting personal information.

Department of Homeland Security's National Strategy to Secure Cyberspace: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. Describes the roles and responsibilities of both public and private sectors in the Department's efforts to secure cyberspace.

OnGuard Online: www.OnGuardOnline.gov. Gives practical tips from the federal government and technology experts on how to guard against Internet fraud, secure your computer, and protect personal information.

ABA Law Practice Management Section: www.abanet.org/lpm/resources/technology.shtml. Contains excellent information for lawyers on identity theft, hacking, viruses, spyware , and more.

ABA Legal Technology Resource Center: www.abanet.org/tech/ltrc. Contains a comprehensive collection of technology resources and information. See the article, "To catch a thief—tips and tools to protect your computer investment," at **www.abanet.org/media/youraba/200806/article10.html**, and also at **www.osbplf.org**.

ABA's GPSolo Technology & Practice Guide: www.abanet.org/genpractice/magazine/2006/jun/index.html. Published by the General Practice, Solo & Small Firm Division, the entire June 2006 issue (volume 23, number 4) is devoted to technological issues such as mobility and security.

Internal Revenue Service: www.irs.gov. IRS news release 2008-88, July 10, 2008, cautions about a new wave of scams using the IRS name in identity theft e-mails (phishing) involving tax refunds and economic stimulus payments.

Oregon Administrative Rule 160-100-0210: www.filinginoregon.com/notary/new_notary_journal_rule.htm. This new rule, effective May 1, 2008, addresses protections for notaries and the clients they serve by helping the notaries comply with the Oregon Consumer Identity Theft Protection Act.