IN BRIEF

OSB Professional Liability Fund

www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

April 2016

Issue 128

What to Do After a Data Breach

A data breach is a traumatizing event, regardless of how it occurs, and last year was a particularly active summer for thieves and scammers. In 2015, Oregon lawyers reported home and office break-ins, stolen laptops and mobile devices, and malware security intrusions. If you experience a data breach, here are the key steps you must take:

- **Contact the Professional Liability Fund.** Call the PLF immediately and ask to speak to a PLF claims attorney, even if you don't have Excess Coverage. Knowing about cyber liability claims enables the PLF to better assist Oregon attorneys with this expanding area of liability. See sidebar on page 10.

- **Contact the Oregon State Bar.** The OSB General Counsel's office can give you advice about the ethical implications of a data breach.

- **Contact an IT expert NOW before you pass go.** The scope of the intrusion may reach beyond your stolen mobile device or the infected computer. Until you know better, assume that all connected devices are part of the data breach. This might include your desktop computer, your assistant's computer, your server, mobile devices used to access your network, and your home computer if you connect remotely to your office. Fixing security issues will require sleuthing, finding a solution, protecting existing data and devices not affected by the breach, testing security solutions, and potentially preserving forensic evidence. Don't try to fix it yourself!

- **Change user names and passwords.** At the first indication of a data breach, you won't know exactly what went wrong – only that your information, or your clients' information, has been compromised. Using an uninfected computer, change user names and passwords for your online accounts. (If you modify your login credentials while a keylogger (a type of spyware) resides on your system, you've made the situation worse by supplying the hacker with your newly replaced credentials.) If necessary, get help from your IT expert.

- **Freeze or place fraud alerts on credit accounts.** A freeze literally locks down your credit. No credit transactions can be authorized until you lift the freeze, temporarily or permanently. Fraud alerts inform you if someone is attempting to obtain new credit in your name. Learn more about credit freezes and fraud alerts at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

- **Protect bank accounts, credit cards, and debit cards.** If banking, credit card, or debit card information was exposed in conjunction with the data breach, you may want to freeze your bank accounts (personal, general, IOLTA), arrange for fraud protection services, or close your accounts altogether. Talk to your banks and credit or debit card providers. If you have automated payments tied to former bank accounts, credit cards, or debit cards, be sure to update your information. This includes payment accounts associated with federal or state court eFiling systems. Continue to monitor statements for unauthorized transactions.

- **File a police report.** Realistically, this isn't likely to help. However, it may be required under the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-646A.628) or the terms of your insurance/coverage policy.

- **Report the breach to your property manager.** If the breach occurred in connection with an office break-in, inform the property manager as soon as possible. Broken windows and locks should be fixed immediately to avoid further loss. If you believe inadequate security may have played a role in the break-in, it may be appropriate to assert a claim against the management or building owner. Research the issue or speak to outside counsel. Document your property loss and consider getting a commitment in writing about security improvements.

- **File claims with commercial carriers.** Submit claims to any applicable insurance carriers: cyber liability and data breach, commercial liability, or others.

- **Report identity theft to the Federal Trade Commission.** If you are the victim of identity theft, file a report with the FTC as soon as possible. Review the FTC website for other steps not discussed here (e.g., reporting a misused Social Security number, removing bogus credit charges, replacing government-issued identification cards). See www.identitytheft.gov/#what-to-do-right-away.

- **Notify clients.** This is never easy, but clients must be informed if confidential information has been compromised. A sample notification letter is available on the PLF website at www.osbplf.org. Select Practice Management > Forms > Client Relations > "Notice to Clients re Theft of Computer Equipment." If you have questions about your ethical duties toward clients, speak to OSB General Counsel (see above). Additionally, client notification may be a statutory responsibility under the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-646A.628).

- **Begin reconstructing files if needed.** Lawyers who are straightforward about an office break-in or theft often find that clients are sympathetic, understanding, and more than willing to help. With a bit of luck, you should be able to reconstruct most or all of your files from your backup or documents supplied by clients.

- **Monitor your credit report.** Check your credit reports at www.annualcreditreport.com for signs of fraud. This is the only official source for free credit reports authorized by the Federal Trade Commission.

- **Monitor Craigslist.** If you believe a thief has posted your property for sale, inform the police.

- **Start using encryption.** Read "Encryption Made Simple for Lawyers" as a starter (ABA GPSolo Magazine, November/December 2012), which is now a book: http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html. Then check out www.lawtechnologytoday.org and the resources from the ABA Legal Technology Resource Center at www.americanbar.org/groups/departments_offices/legal_technology_resources/resources.html. For reviews of encryption products, check out http://www.lawsitesblog.com/. If you want an encrypted password manager – a very good idea – see the top picks for 2016 at www.pcmag.com. Shopping for a new laptop? Don't forget that hard drive encryption is automatically built into the Mac OS. Using Windows OS? Sorry, you'll need to buy your own encryption software. If all this seems overwhelming, talk to your IT expert.

- **Backup, backup, backup!** Online backup services are a great way to automatically back up data. Read more about backup protocols and available resources on the PLF website. Select Practice Management > Forms > Technology > "How to Backup Your Computer" and "Online Data Storage."

- **No cyber liability or data breach coverage?** Buy it! If your claims weren't covered, purchase cyber liability and data breach insurance to protect against future loss – privately or through the PLF as part of our Excess Program. Beginning in 2013, the PLF added a Cyber Liability and Breach Response Endorsement to all Excess Coverage plans. The Endorsement covers many claims that otherwise would be excluded. (See sidebar below.)

- **Stay vigilant.** Fixing a data breach does not mean that scammers or hackers will stop. Watch out for phishing attempts. Don't click on suspicious links in emails, texts, or social media messages. I've written over 20 blog posts on the subject of scams. To find the posts, visit my blog's landing page at http://oregonlawpracticemanagement.com/. In the search box in the upper right corner, enter "scam." You'll also find seven *In Brief* articles on the PLF website at www.osbplf.org. Select Practice Management > Publications > In Brief, and enter "scam" in the search by keyword or year box. See also Jennifer Meisberger, "Sophisticated Scams: Protect Your Clients' Money," *Oregon State Bar Bulletin* (June 2015), and the PLF CLE, "Protecting Your Firm and Your Client from Scams, Fraud, and Financial Loss."

Beverly Michaelis
PLF Practice Management Advisor

Originally posted on September 14, 2015, on http://oregonlawpracticemanagement.com.

Cyber Extortion Coverage Added to PLF Excess Coverage!

We are delighted to announce that 2016 PLF Excess Coverage now includes coverage for Cyber Extortion events under the Cyber Liability and Breach Response Endorsement ("Endorsement") (included in all PLF Excess Coverage plans). There is no additional charge for this coverage enhancement.

Cyber extortion occurs when a business's computer system is attacked and data stored on the computers or networks is rendered unusable because it is encrypted by extortionists. The only possibility for release of that data (unless it is otherwise backed up on a non-infected drive) is through satisfying a payment demand. Another term for this type of virus or attack is ransomware. The PLF is aware of at least one cyber extortion attack made against an Oregon law firm in 2015. That claim would not have been covered under prior Endorsements, nor is there coverage for these claims under the PLF Primary Claims Made Plan.

Under the 2016 Endorsement, the limit available to cover Cyber Extortion claims is $10,000, with a $2,000 deductible. Though cyber extortion demands are often quite small (many would not exceed the deductible), it is important that you notify the PLF of these claims so they can be monitored under the Endorsement. This is particularly valuable if additional claims result from the Cyber Extortion event. We believe this added coverage is of great benefit to Oregon law firms and are pleased to include it in our Excess Coverage for this year.

If you have any questions about the Cyber Liability and Breach Response Endorsement or other aspects of PLF Excess Coverage, please contact Emilee Preble at 503.639.6911 or at emileep@osbplf.org.

Continued on page 4