

# Oregon Law Practice Management

Practice Management Tips for Oregon Lawyers

## What to do After a Data Breach

Posted on **09/14/2015**

A data breach is a traumatizing event, regardless of how it occurs, and this has been a particularly active summer for thieves and scammers.

In the past 12 months, Oregon lawyers have 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:

- 1. Contact an IT expert NOW before you pass go.** The scope of the intrusion may reach beyond your stolen mobile device or the specifically 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 to the problem, protecting existing data and devices not affected by the breach, testing security solutions, and potentially preserving forensic evidence. Don't try to DIY!
- 2. Change vulnerable 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. With your IT expert's help, get access to a secure computer to change vulnerable user names and passwords. [If you modify your login credentials while a [keylogger](#) resides on your system, you've made the situation worse by supplying the hacker with your newly replaced user names and passwords.]
- 3. 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.
- 4. 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.

5. **File claims with commercial carriers.** Submit claims to any applicable insurance carriers: cyber liability and data breach, commercial liability, or others.
6. **Contact the Professional Liability Fund.** If you are an Oregon lawyer, [contact the PLF](#). Beginning in 2013, the PLF added a Data Breach and Cyber Liability Endorsement to all excess coverage plans. The endorsement provides coverage for information security and privacy liability, privacy breach response services, regulatory defense and penalties, website media content liability, and crisis management services. The endorsement covers many claims that would otherwise be excluded.
7. **Contact the Oregon State Bar.** The [OSB General Counsel](#) can provide information about the ethical implications of a data breach.
8. **Report identity theft to the FTC.** If you are the victim of identity theft, [report to the FTC as soon as possible](#). [Review the FTC website for more information](#) [reporting a misused social security number, removing information from credit reports, replacing government-issued identification cards].
9. **Freeze or place fraud alerts on credit accounts.** A [freeze](#) limits access to your credit. No credit transactions can be authorized until you lift the freeze permanently. [Fraud alerts](#) inform you if someone is attempting to use your name. [Learn more about credit freezes and alerts here](#).
10. **Protect bank accounts, credit cards, and debit cards.** If bank or credit card information was exposed in conjunction with the data breach, [freeze your bank accounts](#) [personal, general, IOLTA]; arrange for [fraud protection services](#); or close your accounts altogether. Talk to your banks and credit/debit card providers. If you have automated payments tied to former bank accounts, credit 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.
11. **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](#). 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 step 7 above]. Additionally, client notification may be a statutory responsibility under the [Oregon Consumer Identity Theft Protection Act](#) [ORS 646A.600-646A.628].
12. **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.
13. **Monitor your credit report.** Check your credit reports at [annualcreditreport.com](#) for signs of fraud. [Annualcreditreport.com](#) is the only official source for free credit reports.

+ Follow

## Follow “Oregon Law Practice Management”

Get every new post delivered to your Inbox.

Join 5,656 other followers

Enter your email address

Sign me up

Build a website with WordPress.com


authorized by the [Federal Trade Commission](#).


14. **Monitor Craigslist.** If you believe a thief has posted your property for sale, inform police.
15. **Start using encryption.** Read “[Encryption Made Simple for Lawyers](#)” as a starter, then check out these [resources](#) from the ABA Legal Technology Resource Center. For reviews of encryption products, check out [LawSites](#). [In the navigation pane on the right, scroll midway down the page to Search LawSites.] If you want an [encrypted password manager – a very good idea – see these top picks for 2015](#). Shopping for a new laptop? Don’t forget that hard drive encryption is automatically built into the [MacBook](#). Using Windows OS? Sorry, you’ll need to buy your own encryption software. If all this seems overwhelming, talk to your IT expert.
16. **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.”
17. **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. [See item 6 above.]
18. **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](#). In the search box in the upper right corner, enter “scam.” You’ll also find seven *In Brief* articles on the [PLF website](#). 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](#).


All Rights Reserved [2015] Beverly Michaelis


---


#### SHARE THIS:


 Twitter


 Facebook


 LinkedIn 1


 Pinterest


 Google

 Tumblr

 Email

 Print

 Like



One blogger likes this.

---

#### RELATED

[What Should I Do About](#)

[12 Steps to Take Now if](#)

[Cyber Security and Data](#)

[Lost or Stolen Client Files?](#)

In "Confidentiality"

[Your Laptop is Stolen](#)

In "Confidentiality"

[Breach Response](#)

In "Confidentiality"

This entry was posted in [Confidentiality](#), [Ethics](#), [Financial Management](#), [Fraud Prevention](#) and tagged [Beverly Michaelis](#), [break-in](#), [cyber liability](#), [Data Breach](#), [Oregon law practice management](#), [PLF excess coverage](#), [stolen device](#), [stolen laptop](#), [theft](#) by [beverlym](#).

Bookmark the [permalink](#) [<http://oregonlawpracticemanagement.com/2015/09/14/what-to-do-after-a-data-breach/>].

ONE THOUGHT ON "WHAT TO DO AFTER A DATA BREACH"

[Pingback: The Year in Review – Top Posts in 2015 | Oregon Law Practice Management](#)

