WHAT TO DO AFTER A DATA BREACH

A data breach is an impactful event, regardless of how it happens. No matter how much you try to prevent a breach, everyone will likely experience one at some point in their career. If you do sustain a data breach, you can take the following steps to mitigate the damage:

1. **Contact an IT expert** – An IT expert can help determine the extent of the breach and possibly assist with preventing further damage and exposure. If you already have an IT professional who is knowledgeable about data breaches, contact them. Otherwise, work with IT people who have experience with data security and can properly respond to resulting issues. Do not attempt to navigate or fix the issues yourself. They can also help you prepare and implement your Incident Response Plan, as discussed below.
2. **Implement your Incident Response Plan (IRP)** – An IRP is a set of protocols for managing the aftermath of a security incident, including a cyberattack or a lost or stolen device. The purpose is to minimize the effects of breaches through a swift and thorough response. Work with your IT expert to create an IRP that fits your firm's needs.
3. **Contact the Professional Liability Fund (PLF)** – Call the PLF immediately and ask to speak to a practice management attorney. We will provide you with guidance and resources. Claims resulting from a data breach are excluded in the PLF Primary Coverage Plan but are covered if you have PLF Excess Coverage. A Cyber Liability & Breach Response Endorsement is automatically included with all PLF Excess Plans.
4. **Notify your cyber liability insurer** – If you have cyber liability coverage through a commercial carrier, notify them of the breach and cooperate with their policy requirements.
5. **Notify your business insurance carrier** – Notify your business insurance carrier if your policy requires it.
6. **Get legal ethics advice** – Get advice about possible ethical implications of a data breach. Contact a private legal ethics attorney or the Oregon State Bar (OSB) General Counsel's Office. Note that any communications with the OSB are not confidential.
7. **Inform clients** – You must inform your clients if their confidential information has been compromised. Communication should be clear, concise, and informative. See the *Notice to Clients re Theft of Computer Equipment.* Go to the PLF website, www.osbplf.org > click on the Services tab > CLEs & Resources > Practice Aids tab > search by category or by document name. If you have questions about your ethical duties to clients, speak to OSB General Counsel. Additionally, client notification may be a statutory responsibility under the Oregon Consumer Identity Theft Protection Act (ORS 646A.600- 646A.628).
8. **Review the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-646A.628)** – Passed by the legislature in 2007, this law applies to lawyers who store certain types of personal client information and requires notices to be sent to clients in the event of a breach. It also requires reasonable safeguards in handling and disposing of the client information.
9. **Inform 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 building security might have played a role in the break-in, it may be appropriate to file a claim with the building's management or owner. Research the issue or speak to outside counsel. Document your property loss and consider getting a commitment in

writing about security improvements.

10. **Contact the Federal Bureau of Investigation (FBI)** – Depending on the type of incident, the FBI may be able to assist with filing reports, investigating the situation, and directing you to resources for preventing future breaches. Go to https://www.fbi.gov/.
11. **Report identity theft to the Federal Trade Commission (FTC)** – If you are the victim of identity theft, file a report with the FTC as soon as possible. Go to the FTC website at https://www.identitytheft.gov/#/ for more information.
12. **Report to the Internet Crime Complaint Center (ICC)** – You should also report any internet-related crimes to the ICC at https://www.ic3.gov/.
13. **File a police report** –You should report the breach to your local police station. Filing a police report may also be required under the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-646A.628) or the terms of your insurance policy.
14. **Change all usernames and passwords** – You may not know the extent of the breach, but it is important to change all your usernames and passwords—no matter how minor or limited the breach may seem. This could be an extensive task since we all use many devices and programs, but it is important. Using a device that has not been infected, change the usernames and passwords for all your accounts.
15. **Freeze or place fraud alerts on your credit** – A freeze locks your credit until you lift the freeze. Fraud alerts notify you if someone is attempting to obtain credit in your name. This would only protect your personal credit. Learn more about credit freezes and fraud alerts at https://consumer.ftc.gov/articles/what-know-about-credit- freezes-fraud-alerts.
16. **Protect bank accounts, credit cards, and debit cards** – If any financial information was exposed in conjunction with the data breach—whether business or personal—you may want to freeze your bank accounts (personal, business, IOLTA), arrange for fraud protection services through your bank such as Positive Pay, or close the accounts altogether. Talk to your banks and card providers to determine the necessary steps. If you have automated payments tied to any account, be sure to update the information. Continue to monitor statements for unauthorized transactions.
17. **Monitor your credit report** – Check your credit reports at www.annualcreditreport.com for signs of fraud on your personal credit. This is the only official source for free credit reports authorized by the Federal Trade Commission.
18. **Reconstruct lost files** – Contact your IT person for assistance with reconstructing files. They may be able to recover data and locate backups. With a bit of luck, you may be able to reconstruct most—or all—of your files from your backup or documents supplied by clients and your IT person.
19. **Evaluate your IRP and perform a risk assessment** – After you've recovered from a data breach, discuss lessons learned to give all involved the opportunity to determine the effectiveness of each step taken in response to the incident. Consider ways to enhance your firm's data security and avoid future breaches. See the *Checklist to Prevent and Prepare for a Data Breach.* Go to the PLF website, www.osbplf.org > click on the Services tab > CLEs & Resources > Practice Aids tab > search by category or by document name.

WHAT TO DO AFTER A DATA BREACH
IMPORTANT NOTICES