Law Society of British Columbia

Practice Resource[1]

Lost or stolen briefcase? Cyber attack? What to do if your practice records have been compromised

If you have lost custody or control of your electronic or physical records[1], including personal or confidential client information, for any reason (misdirected correspondence, lost or misplaced records or electronic devices, theft, a cyberattack, or otherwise), consult your security breach response plan. If you do not have a plan, below is a short list of procedures to consider (not a substitute for a detailed plan). Determine the applicability of the procedures and their order in context. Not every procedure may be applicable to every situation.

1. Establish your response team, its responsibilities and priorities, including a communication plan to staff and others.

2. Contact a Law Society practice advisor if you have questions regarding your professional obligations pursuant to the *BC Code*, including sections 3.3 (Confidentiality) and 7.8 (Errors and omissions) and Law Society Rules 3-74 (Trust shortage) and 10-4 (Security of records). Your clients will need to be informed if their records have been compromised or lost. Contact a practice advisor by email at practiceadvice@lsbc.org or by phone at 604.443.5797. In the case of a cyber breach, only use email if your IT professional or Coalition, Inc. says that is it safe to do so.

3. Report to the Lawyers Indemnity Fund (LIF) immediately if the lost records or missing information relate to a client file with an imminent transaction or proceeding, or a loss of trust funds: Report a claim to LIF.

4. Report to LIF's cyber program insurer, Coalition, Inc., immediately for both physical and technological privacy or data breaches: Report a claim to Coalition. The program coverage includes a breach coach or privacy lawyer (two hours free) to advise on regulatory compliance, notifying clients and third parties, credit monitoring costs, data restoration costs, network interruption costs, ransomware and more. LIF's website has more information about your cyber coverage: Your Cyber Coverage | LIF.

5. You may have additional privacy and data breach coverage from another insurer, so you should also contact your broker.

6. Contact your IT professionals to work with Coalition's security team.

7. Contact LIF to discuss recreating files if physical records are lost and information is missing.

8. Contact your financial institutions if bank accounts and credit cards are at risk.

---

[1] A "record" may include accounting records and supporting documents (trust account, general account. cash transaction and billing records), client identification and verification information and documents, metadata associated with electronic records, and client file documents, whether in paper or electronic form.

9. Send Rule 10-4 (Security of records) reports to the Executive Director c/o Director, Intake, Early Resolution & Practice Standards (professionalconduct@lsbc.org). Send Rule 3-74 (Trust shortage) reports to the Executive Director c/o Trust Assurance (trustaccounting@lsbc.org). Sample letters for reporting trust shortages are in Appendix C of the Trust Accounting Handbook. If your IT professional or Coalition says that it is not safe to use email, you can send your reports by Canada Post or courier to the Law Society of British Columbia, 845 Cambie Street, Vancouver, BC V6B 4Z9).

10. Report to your local police (optional but may be a requirement by some insurers) and to the Canadian Centre For Cyber Security (also optional).

11. Update or design your response plan based on what you have learned.