DATA BREACH REPORTING: WHEN U.S. LAWS APPLY TO CANADIAN COMPANIES

Smarter Way to Cross Blog Archives
March 26, 2013

From stolen laptops and missing hard drives to nefarious parties exploiting security weaknesses, companies need to have policies in place when, not if, a data breach occurs. Every data breach policy should include guidance about how a data breach is reported to affected users. But in today's highly connected world it is common for many of these users to be located internationally—including in the United States. As a result, Canadian companies and counsel should know and comply with U.S. requirements when reporting a data breach.

The U.S. government enacted several industry-specific privacy laws with data breach notification provisions. These industry-specific laws include:

- Health Information Technology and Economic and Clinical Health "HITECH" Act (health care),
- Federal Information Security Management Act "FISMA" (law enforcement and security)
- Gramm-Leach-Bliley Act (financial institutions)

However, the United States lacks a comprehensive federal data breach notification law, and instead relies on a patchwork of state laws.

Generally, the affected user's residence determines which state law must be followed. For example, the New York data breach notification law requires that any company engaged in business with New York residents must notify those residents in the event of a breach of private information, regardless of whether the company is based outside of New York State.

In further support of this idea, the American Bar Association (ABA) held a panel discussion on U.S. and Canadian data breach notification laws in 2011. The panel argued that under both Canadian and American law, it is likely that Canadian companies would be subject to state data breach notification laws:

Canadian businesses with…American customers… may have a statutory obligation to notify their foreign customers in the event of a data breach. […] The [U.S. data breach] laws generally apply to custodians of information for the residents of a particular state; however, there is no such limitation regarding the location of the custodian."

Likewise, the panel argued that Canadian businesses with American customers may be also subject to state data breach laws under Canadian law:

[I]n conflict of laws issues, a Canadian court could find sufficient connections between an American individual and a Canadian information custodian to enforce in Canada a judgment under one of the American statutes." *Id.*

Though this question has not been litigated in New York State (as of this writing) or elsewhere, and is therefore open to interpretation, case law governing personal jurisdiction in the United States seems to suggest that international companies are covered by N.Y. Gen. Bus. Law § 899-aa. Canadian companies in particular may be subject to state data breach laws by

Canadian conflict of law precedence.

Therefore, Canadian companies and counsel should know and comply with U.S. data breach reporting requirements when U.S. customers are involved. In many U.S. states, time is of the essence when reporting a data breach (days not months!), so it is critical that client and counsel discuss these issues and create an action plan before a data breach occurs.

Along these lines, it is important to have a written and up-to-date post-breach response plan that is mindful of what regulations, statutes, and contracts cover post-breach obligations. These types of plans should be ready and tested *before* a breach happens.