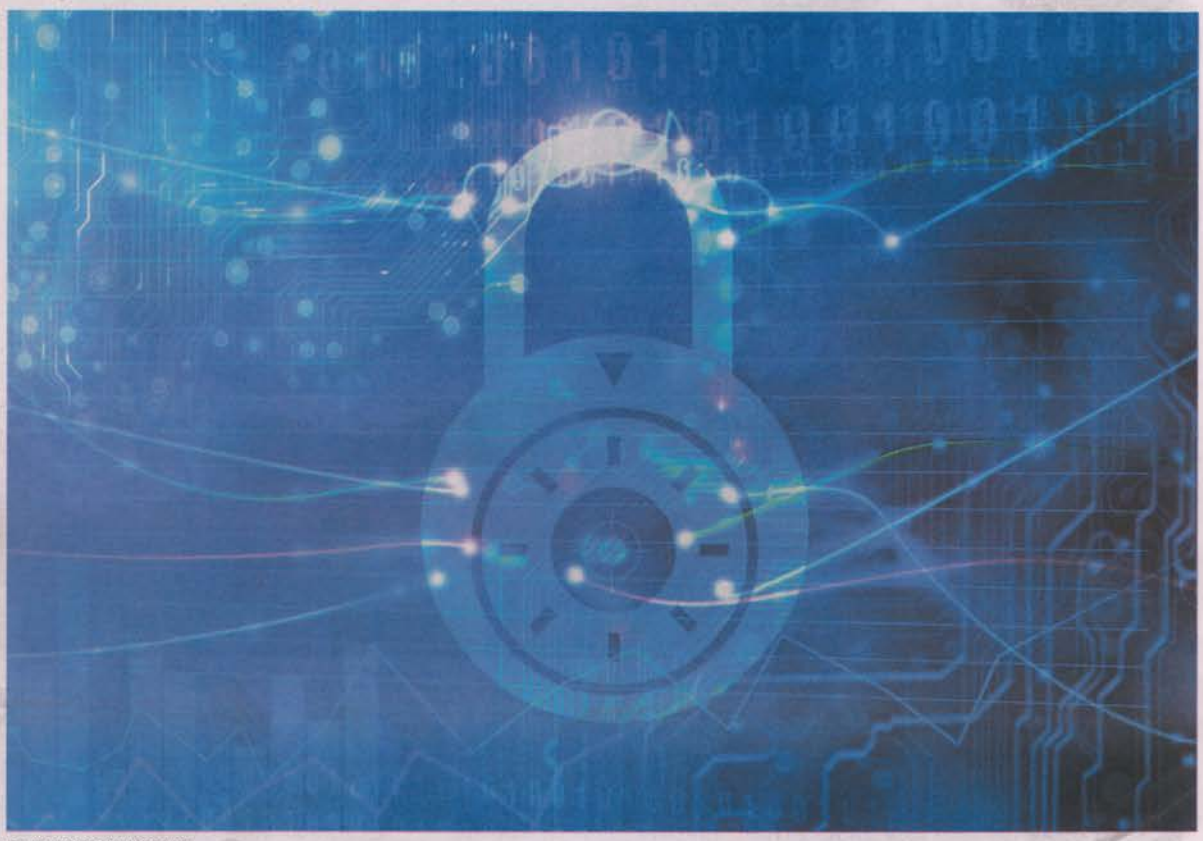
Focus INFORMATION TECHNOLOGY

Notification after a data breach

U.S. reporting requirements cross borders

Jordan Walbesser



KALAWIN / ISTOCKPHOTO.COM

A patchwork variety of reporting requirements have emerged as governments and advocacy groups demand greater transparency after a data breach. However, the international nature of the Internet creates multi-jurisdictional requirements. As a result, Canadian clients with U.S. customers should know, and comply with, U.S. requirements when reporting a data breach.

The importance of this is increasing as data breaches become an all too familiar occurrence. For example, reported data breaches in the U.K. have risen by more than 1,000 per cent in the last five years. 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 how a data breach is reported to affected users. However, in today's highly connected world it is common for many of these users to be located internationally—including in the U.S. This article focuses on U.S. laws applicable to extra-territorial data breaches, but other national laws may also apply.

The U.S. government enacted several industry-specific privacy laws with data-breach notification provisions. These industry-specific laws include the *Health Information Technology for Economic and Clinical Health (HITECH) Act* (health care), *Federal Information Security Management Act* (FISMA) (law enforcement and security), and the *Gramm-Leach-Bliley Act* (financial institutions).

However, the U.S. lacks a comprehensive federal data breach notification law. Instead, 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. (A list of the applicable U.S. state laws can be found at: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.)

Generally, the affected user's residence determines which state law must be followed. For example, the New York data breach notification law (*N.Y. Gen. Bus. Law § 899-aa*) states:

> Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

In other words, New York requires that any company engaged in business with state 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.

Although "conducts business" is not defined within the law, New York courts generally define conducting as a "purposeful activity—'some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws'" (*McKee Elec. Co. v. Rauland-Borg Corp.*, 20 N.Y.2d 377, 382 (1958)).

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 also be subject to state data-breach laws under Canadian law: "in 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," the panel noted. Though this question has not been litigated in New York or elsewhere, and is therefore open to interpretation, case law governing personal jurisdiction in the United States, as well as the opinion of the ABA, seem to suggest that international companies are covered by *N.Y. Gen. Bus. Law § 899-aa.2*. Canadian companies in particular may be subject to state data breach laws by Canadian conflict of law precedence.

Therefore, Canadian clients with U.S. customers should know, and comply with, U.S. data breach reporting requirements. In many 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. Handling a complex issue such as a data breach in a timely and proper manner will repair consumer confidence for your client, and in turn, keep your client happy.

Jordan Walbesser, a lawyer at Hodgson Russ LLP, concentrates his practice in intellectual property law, with a focus on patents and business methods. He is also well versed in software, cloud computing, social media, and peer-to-peer networking issues.

We want to hear from you!
Send us your verdict:
comments@lawyersweekly.ca

> "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.
>
> **Jordan Walbesser**
> Hodgson Russ LLP