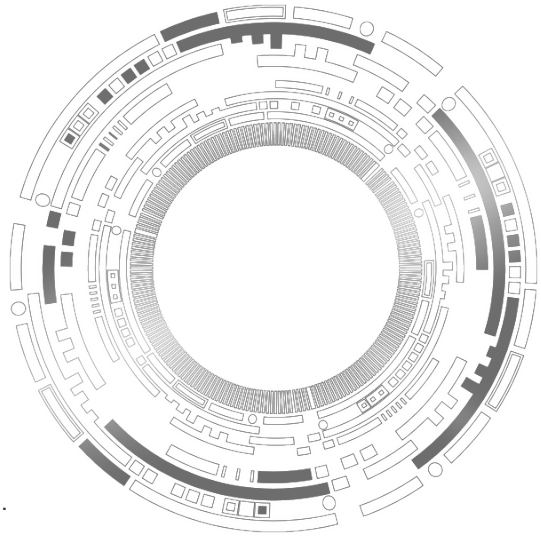
BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes
CANADIAN LAWYERS

TRENDS



TECHNOLOGY

Throughout the remainder of 2016 and into 2017, we will be providing key insight into current trends across different industries. The first in our series concerns technology, with a particular focus on financial technology (fintech) and cybersecurity.

1

Peer-to-Peer Pressure: Next Steps for Canadian Fintech

It's likely we will see more legislation for fintech in 2017. The Canadian Competition Bureau's fintech market study is due to be published in the spring and will include an exploration of whether there is a need for regulatory reform to promote greater competition, while maintaining consumer confidence in the sector.

Countries such as the United Kingdom have already pioneered pro-innovation fintech regulation, including the introduction of such ideas as a "regulatory sandbox" – a safe space to test out innovative financial products and services without fear of regulatory reprisal – while Australia and China have also shown likeminded approaches to the sector.

Like those countries, Canada is seen as being a global fintech hub – with renowned national financial institutions pioneering projects with blockchain technology and fintech startups increasingly popping up across major cities. Regulation, however, is not moving at quite the same pace.

There was something of a milestone in September of this year, when the Ontario Securities Commission (OSC) decided to grant an exempt market dealer registration to an online lender, Vault Circle Inc. This was a significant step forward for peer-to-peer lending platforms in Ontario, which are currently subject to strict securities legislation. The exempt market dealer licence for Vault Circle Inc. means it now has regulatory approval to participate in the accredited investor marketplace.

This was followed in October by a cross-Canada dealer registration for another online lender, Loop Securities Inc., which relied upon a heavily customized offering memorandum exemption.

A sign of things to come? The next year will show us whether Canada will continue to proceed with caution, or encourage the innovation that has potential to transform the financial services industry.

2

Data Privacy and Security

The rapid pace of growth for fintech companies needs to be balanced by an informed approach to data privacy and security.

The nature of fintech organizations means the data they hold is often highly sensitive personal information such as date of birth, social insurance number, bank account details, online banking credentials and credit score. For a relatively new fintech company, a data breach could have a devastating impact on customer trust and investor confidence.

Fintech companies also face privacy challenges when expanding a product or service offering developed for one jurisdiction to another jurisdiction with different privacy and data protection rules. For example, when launching in Canada, many U.S. offerings need to be modified to account for Canada's broad definition of personal information.

Yet there are real opportunities for the newer fintech companies regarding data and privacy. In fact, they may have a distinct advantage over existing financial services providers, since they can build privacy protective controls and security safeguards into the technology as it is developed, rather than having to fit them into existing processes and systems retroactively.

For more on this, read *Big Data, Big Risk? Privacy and Security Tips for Fintech Companies.*

3

Meet the Cyber-Whistleblower

With the average cost of a data breach totalling millions of dollars, it's no surprise that many organizations will be ensuring there is an increased focus on cybersecurity over the coming year. But the cost of cybersecurity could be even more than many organizations are anticipating, due to a recently introduced law on whistleblowing.

The OSC's *Whistleblower Program* states whistleblowers may be able to receive monetary rewards of up to C$5-million for providing information about violations of securities laws to the OSC. The policy also provides for the payment of rewards of up to C$1.5-million even when the OSC has not recovered any funds from wrongdoers, and does not require whistleblowers to use available internal reporting mechanisms.

This could have a significant impact on cybersecurity for organizations in Ontario. For example, a corporation that has issued securities to the public (a reporting issuer) is required under securities legislation to publicly disclose any material changes. This includes a change in the business, operations or capital that would reasonably be expected to have a significant effect on the market price or value of any of its securities.

If a data breach were to result in such a change for a reporting issuer, and remain unreported, then the cyber-whistleblower could directly report the violation to the OSC and potentially receive a significant financial reward as a result.

It's therefore important that businesses in Ontario have a comprehensive understanding both of how to keep their data secure and the impact a cyber-whistleblower could have on their business.

4

Offence – The Best Form of Defence?

Offensive Counter Measures (OCMs) are a method of turning the tables on a cyber-attacking assailant. They cover everything from an organization identifying the origin of attacks on its system to stealing back what was taken from them (hacking back).

Examples of OCMs include photographing the hacker using their own system's camera, physically disabling or destroying the hacker's own computer or network, or gathering intelligence by implanting malware in the hacker's network.

OCMs are, by their very nature, a high-risk strategy. Operational risks include unintentionally targeting innocent people (hackers frequently route attacks through innocent parties to mask their identities) and inciting escalation from the hacker, potentially worsening the data breach that has already taken place.

There are also numerous legal risks, including potential breaches of the *Criminal Code*, statutes including *Canada's Anti-Spam Legislation* and the *Personal Information Protection and Electronic Documents Act* (the federal privacy law for private-sector organizations), as well as possible civil liability.

However, the law surrounding OCMs remains in flux. Without decisions relating to the issues mentioned above, there is considerable uncertainty on how potentially relevant provisions or claims for intrusion upon seclusion will be enforced.

For further information, please contact Christine Ing or any other member of our Technology group.

Blakes