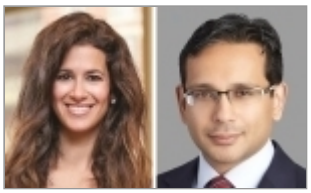
THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Business

Digital disruptor: The legal challenges of 'open banking'

By **Sharon Bauer and Imran Ahmad**



Sharon Bauer and Imran Ahmad

(February 26, 2018, 9:22 AM EST) -- There is little doubt that in an increasingly digital world, personal data has become a valuable commodity. Financial institutions (FIs) are in a unique position since they collect and process vast quantities of customer data, including, among other things, spending trends, credit history and borrowing information. Typically, this information is not readily shared with customers or other FIs.

One of the challenges with this "closed" model is that other financial service providers cannot effectively analyze the data, potentially stifling the development and rollout of innovative products and services to consumers.

"Open banking" promotes the concept that financial data should be interconnected between FIs and other financial service providers like financial technology (fintech) firms. Once financial data is shared, through an application programming interface (API), FIs and the like will be able to analyze that data and provide customers insightful financial information that they otherwise would not get. For example, a fintech startup may use artificial intelligence or machine learning to advise its customers that the funds used to pay off credit card bills each month would be better spent paying off mortgages. Similarly, within seconds, data can be analyzed to determine which FI offers the best interest rate in light of the customer's criteria.

Proponents of open banking argue that innovative products create competition among fintech firms and FIs, which ultimately improves customer service and equally benefits the financial industry.

Asia, and more recently the EU, have legislated FIs to share data with each other and fintech firms. Open banking has been viewed as a positive disruptor to an otherwise stagnant financial industry. However, highly sensitive personal data shared between multiple parties raises privacy and security concerns. As Canadian FIs put their mind to open banking, they need to consider national and international frameworks within which they must comply.

The paradox of open data and privacy

While the concept of open banking promotes the distribution of data among multiple parties, privacy legislation instills limits on this practice. As gatekeepers of sensitive customer data, FIs, including fintech firms, have a greater responsibility to protect customers' privacy.

In Canada, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs how organizations can collect, use and disclose personal information. API developers should implement Privacy and Security by Design principles when designing APIs, keeping privacy regulations at the forefront of their design matrix, especially at the conceptualization stage.

Moreover, developing a comprehensive data management practice is essential. As part of that plan, API developers need to consider the location of their customers, third party vendors and cloud service providers. If API developers are engaging in cross-border data transfer, they need to adhere to data protection legislation and applicable guidelines from Canadian regulators and different jurisdictions so that they are not inadvertently breached, resulting in significant fines.

Organizations must also be prepared for a potential privacy breach, which may result in a "real risk of significant harm" to their customers, who must be notified as soon as "feasible." An incident response plan addressing detection, response to, and reporting of a privacy breach is vital and will soon be mandatory.

Security risks in a cyberattack

The key threat to open banking is its security vulnerability, which can undermine the entire open ecosystem. As a general proposition, FIs are at a higher risk of cyberattacks given the financial windfall for hackers. This risk increases when new connections are made between various entities, including API developers.

Startups often want to be the first in market to increase sales and traffic. In doing so, and perhaps due to limited funding, fintech startups may forgo or delay security checks and balances, overlooking vulnerabilities to their service offering. Developers need to keep Privacy and Security by Design in mind when designing their product. In doing so, developers will become aware of security vulnerabilities allowing them to patch and update their system as they develop it. Encryption of data, audit trails and data minimization is critical to the design of a product.

Amendments to PIPEDA relating to breach notification, expected to come into force this year, will introduce new breach notifications and reporting provisions. Accordingly, FIs and API developers should have a comprehensive incident response plan in an event of an attack. The plan should address, among other things, steps to take once a cyberbreach occurs, ways to eliminate cyber threats and steps to restore data and the operating systems. All security-related decisions should be documented as they will be scrutinized by regulators and litigants should a breach occur.

As organizations become more secure, hackers become more sophisticated. The link between these two parties is the customer. Phishing attacks are one of the more common cyberattacks. In addition to educating their customers, FIs need to ensure they have proper safeguards, such as Know Your Customer and authentication procedures to protect not only their customers but their entire network.

A possible security solution may be blockchain technology which has been recognized as an open and distributed network that is secure. However, it is too early to tell whether blockchain will be the answer to open banking's security challenge. Blockchain, of course, comes with its own challenges such as the inability to identify and recover losses arising from cyberattacks on exchanges or crypto wallets.

Open banking is an attractive disruptor to the traditional financial industry. It allows individuals to feel empowered by having control over their financial data, which further encourages the financial industry to be more transparent, competitive and innovative. Privacy and security implications must be addressed and taken seriously given the highly sensitive data at the core of the system. Any vulnerability can result in the breakdown of this transformative and open ecosystem.

Sharon Bauer is a partner at Wolfe Lawyers *and can be reached at* sbauer@wolfelawyers.com. *Imran Ahmad is a partner and national leader of the cybersecurity law practice at* Miller Thomson LLP *and can be reached at* iahmad@millerthomson.com.

Photo credit / Mikko Lemola ISTOCKPHOTO.COM