mcmillan

ACC Association of Corporate Counsel ONTARIO

Cybersecurity, Blockchain and Cryptocurrencies – Where Law and Technology Intersect

October 2, 2018

McMillan LLP

Vancouver
Calgary
Toronto
Ottawa
Montréal
Hong Kong

mcmillan.ca

Video Recording

This presentation will be posted on
mcmillan.lawcast.tv/

mcmillan

Blockchain Technology: Legal Implications for Privacy, Data Protection and Data Processing

A. Max Jarvie, McMillan LLP
October 2,2018

McMillan LLP

Vancouver
Calgary
Toronto
Ottawa
Montréal
Hong Kong

mcmillan.ca

Distributed Ledgers Generally

- Formally: A distributed ledger is a **consensus-based data collection** that is **replicated** and **synchronized** across **multiple nodes** or sites.
- Could be instantiated in different media using different methods.
  - Paper + people
  - Blockchain
  - Directed acyclic graph (DAG)

Types (different axes) of Distributed Ledger Technologies

- Permissionless / Permissioned
- Mined / not mined
- Blockchain / Directed Acyclic Graph (DAG) / ?

Can mix and match, thus:

- Bitcoin: permissionless + mined + blockchain
- IOTA: permissionless + not mined + DAG
- Ripple: permissioned + not mined + blockchain

Distributed Ledger Technologies: Value Proposition

- "a distributed yet provably accurate record" (Kevin Werbach, 'Trustless Trust', 2016)
- Utility arises where there are multiple parties that do not trust each other but need to share information
- Advantages (in principle) articulated Satoshi Nakamoto's Bitcoin whitepaper of 2009:
  - Transparency
  - Immutability*
  - Low transaction costs*
  - Decentralization*

*sort of…

Decentralization of what?

- Data
- Data validation
- Access
- Control

Blockchain

- A blockchain is a distributed ledger that consists of:
  - A list/log file [**data collection**] that is
  - partially or fully replicated and synchronized [**replicated + synchronized**]
  - across a distributed network of nodes [**multiple nodes**] and
  - the nodes collectively validate and maintain a growing list of transactions parceled into an immutable chain of blocks [**consensus-based**]
- Transactions are initiated by actors interacting with the network of nodes

Blockchain Background: How it works

- Each user has one or more accounts / addresses (in cryptocurrencies, the accounts have a balance of tokens)
  - Each user controls the private key associated with an account / address
- Users create transactions
  - In pure cryptocurrencies, the substance of the transaction is spending tokens (effectively, moving tokens from one account to another)
  - In blockchains with additional functionality, the substance of the transaction could be spending tokens (Bitcoin), publishing smart contracts (Ethereum), publishing blog posts (Steemit)
- Transactions may be coupled with a transaction fee the participants are willing to pay to a transaction validator
- The transaction is broadcast to the network
- A node that is actively validating ('mining') collects transactions in its memory pool
- Sufficient transactions to fill up a block are selected and block validation begins
  - Transactions may be selected algorithmically from the pool based on the transaction fee attached

Blockchain and Privacy Law

- Personal Information Protection and Electronic Documents Act ("**PIPEDA**")
  - Does it apply? (s. 4(1))
    - Applies to organizations
    - in respect of personal information that
      a. the organization collects, uses or discloses in the course of commercial activities; or
      b. is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.
    - "Organization includes an association, a partnership, a person and a trade union" (s. 1)
    - "Personal information means information about an identifiable individual" (s. 1)

PIPEDA Pitfalls

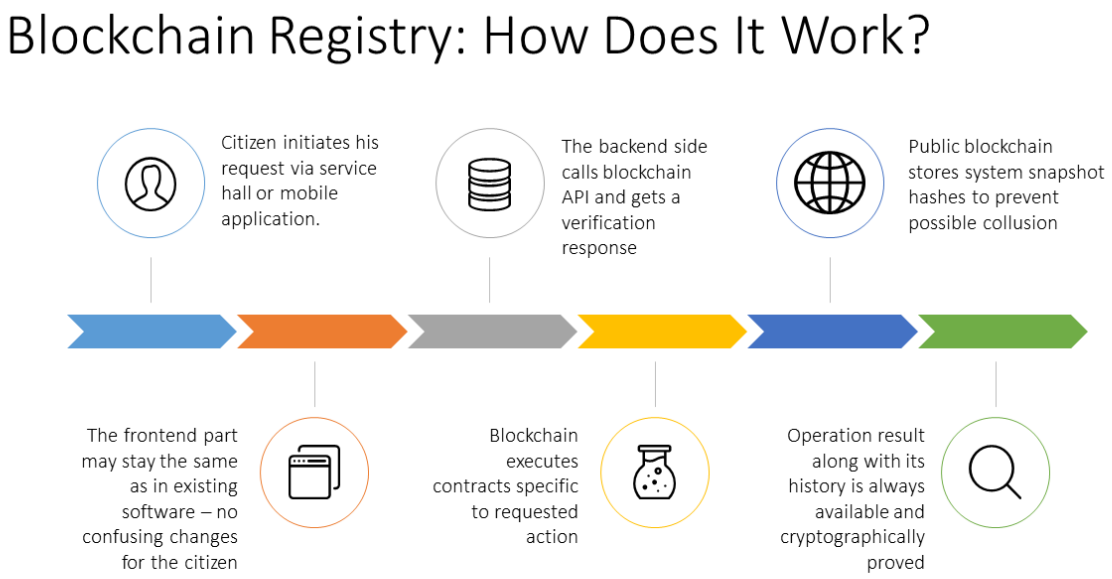
- Accountability (PIPEDA Principle 1):
  - *4.1.3: An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*
  - How do PIPEDA concepts of control, custody, and possession apply to blockchain technology?
    - PIPEDA, like other data protection legislation, was written on the assumption that centralized services control access rights to data, which is more or less the opposite of how permissionless blockchains operate and, more generally, goes against one of the the core value propositions of blockchain technology .
  - Are network nodes third party processors?

PIPEDA Pitfalls cont'd.

- Limiting use, disclosure, and retention (PIPEDA Principle 5):
  - Distribution across multiple nodes: in tension with limiting use and retention
- Safeguards (PIPEDA Principle 7): protection of personal information: blockchain transaction data are not encrypted (unless steps are taken)
  - Encrypted personal information is still personal information – obligations under PIPEDA are still engaged
- Openness (PIPEDA Principle 8): Being transparent with individuals about data handling practices, including where their data is being processed
  - Challenging to provide specifics, particularly on permissionless blockchains
- Individual access (PIPEDA Principle 9): an individual's right to amend information
  - public blockchain transaction data are, by design, effectively immutable; even on permissioned blockchains, removing or amending data would be difficult and inefficient

Possible Solutions?

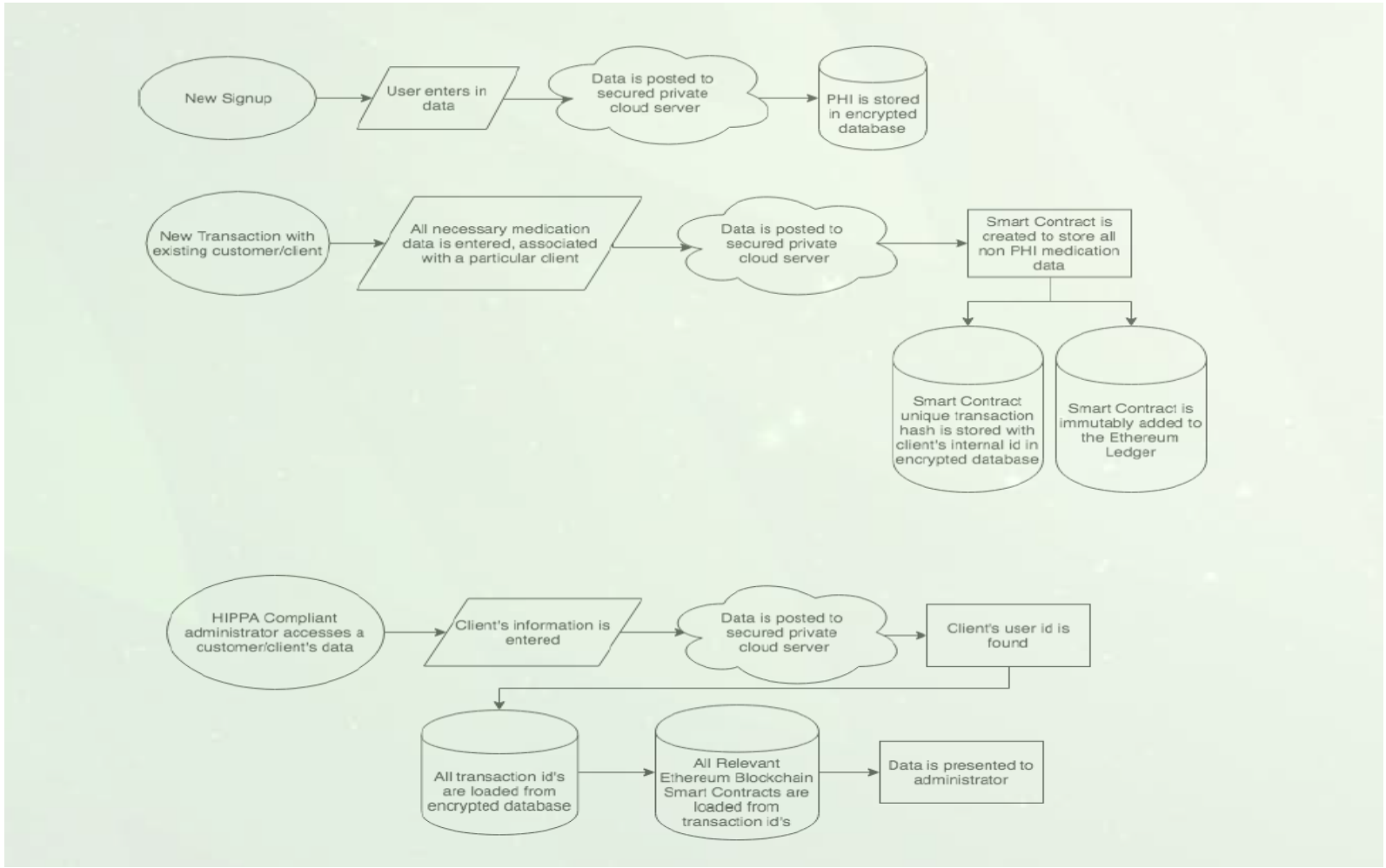
- Keep information on traditional database (or private, permissioned blockchain), inject hashes of the information onto a public blockchain
  - The Republic of Georgia's land registry: saves a hash of the system at a particular time into the bitcoin blockchain



Possible solutions cont'd.

- Use a permissioned blockchain & as added protection, keep key personal information off the blockchain, linked to numerical account IDs to track transaction flows.
  - CanaPass EMR / EHR:
    - "Based on Ethereum's platform, CanaPass' HIPAA and PIPEDA-compliant system records key medical data in blocks on a distributed ledger. Each patient's CanaPass account includes its own private cryptographic key that is used to identify and decrypt the associated private information from the distributed ledger. This is similar to the way a blockchain wallet works, but instead of keeping track of tokens or digital assets, it is used to track and store data such as the patient's lab results, medical reports, etc."
    - "All sensitive patient data storage exceeds HIPAA and PIPEDA requirements; Since only the hash value of sensitive data is stored on the blockchain, data can only be decrypted with the private key of that account."

Canapass


New Signup
User enters in data
Data is posted to secured private cloud server
PHI is stored in encrypted database
New Transaction with existing customer/client
All necessary medication data is entered, associated with a particular client
Data is posted to secured private cloud server
Smart Contract is created to store all non PHI medication data
Smart Contract unique transaction hash is stored with client's internal id in encrypted database
Smart Contract is immutably added to the Ethereum Ledger
HIPPA Compliant administrator accesses a customer/client's data
Client's information is entered
Data is posted to secured private cloud server
Client's user id is found
All transaction id's are loaded from encrypted database
All Relevant Ethereum Blockchain Smart Contracts are loaded from transaction id's
Data is presented to administrator

mcmillan

ACC Association of Corporate Counsel ONTARIO

Selected Canadian Perspectives on ICOs

by Kosta Kostic

October 2, 2018

McMillan LLP

Vancouver
Calgary
Toronto
Ottawa
Montréal
Hong Kong

mcmillan.ca

Introduction – Basic Concepts

- "What is '*The Blockchain*' and how can I '*tokenize*' something and profit from an ICO?"
  - "The Blockchain" does not exist, rather **"Blockchain"** represents an enabling underlying technology that can be used to implement a number of products or services. As technologies are not typical regulated, it is those products or services that are built upon a blockchain that should be subject to regulation.
  - From Wikipedia: A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority (i.e. 50+1% attack).
  - The term **"ICO"** can include a distribution of coins or tokens also referred to as an initial token offering, token generation event, or token distribution event.

CSA Regulatory Sandbox

- In February 2017, the Canadian Securities Administrators (CSA) launched a regulatory sandbox initiative. The purpose of the sandbox is to foster novel businesses and innovation by providing a harmonized regulatory approach across Canada. Through it, the CSA members (i.e. Ontario Securities Commission, British Columbia Securities Commission, Autorité des marchés financiers (Québec)) consider applications for registration and/or exemptive relief on a coordinated and flexible basis.
- To date, the Sandbox has granted varying degrees of exemptive relief from either the **prospectus requirement** or the **registration requirement** (and in one case both) to 8 businesses – one crowdfunding platform oriented to sophisticated or "accredited" investors (AngelList LLC), two companies seeking funding through ICOs (Impak Finance and Token Funder) and five investment fund mangers for cryptocurrency investment funds.
- The Sandbox initiative led to the publication of CSA Staff Notice 46-307 *Cryptocurrency Offerings*, to provide guidance to cryptocurrency businesses on potential Canadian securities law considerations and recently published CSA Staff Notice 46-308 – *Securities Law Implications for Offerings of Tokens* to provide additional practical guidance on when coins or tokens could be characterized as securities.
- There is still a lot of confusion among entrepreneurs surrounding the applicability of securities laws with respect to ICOs. This frequently results from the confusion between what is a utility (functional) token versus a security token.

Exemptive Relief Decisions for ICOs

- Since August 2017, the CSA has granted exemptive relief to two businesses proposing to conduct **ICOs**. The relief granted consisted of:
  - in both cases, **dealer registration relief** that provided for the ICO coins or tokens to be distributed using prospectus exemptions
  - in one case, **prospectus relief** to facilitate the tokens' circulation (or limited resale) in a defined ecosystem as a form of currency [Impak Finance]
- The relief allowed these novel businesses to raise capital with tailored restrictions. The prospectus relief granted to Impak Finance demonstrates the regulators' willingness to consider a flexible approach to tokens with unique characteristics, if investor protection concerns are adequately addressed (including know your client and suitability requirements).
- Unfortunately, to date, no project has received unconditional relief for the resale of the coins or tokens, which is essential to enable trading on a virtual exchange

ICO as a distribution of "securities"

- In CSA Staff Notice 46-307, the CSA noted that in many cases the determination of whether a coin or token is a **security** will be based on whether it is an **investment contract**.
- The relevant case law, including Pacific Coast Coin Exchange v. Ontario (Securities Commission), [1978] 2 S.C.R. 112 as well as subsequent judicial and administrative decisions, refers to a **four-pronged test** for finding an investment contract if there is: **1)** an investment of money, **2)** the investment is made into a common enterprise, **3)** an expectation of profit, and **4)** such profit to come significantly from the efforts of others. This is analogous to the infamous "Howey Test" elaborated in the US supreme court in 1946.
- As pointed out by the BCSC, stakeholders have identified the following variables as potential factors to consider whether an investment contract exists with a given ICO:
  - **Whether a secondary market exists and is available for a coin or token.** For example, tokens compliant with the Ethereum standard ERC-20 are structured in a way that makes them readily tradable on many cryptocurrency exchanges. This may increase the potential for speculation in a token.
  - **Whether a buyer is intending to use a coin or token for a utility function or speculation.** Sellers of tokens often purport that there is a "utility" function to the token that constitutes the reason for its purchase, that is separate from its potential function as an investment. However, tokens are often traded from the time they are sold, indicating that buyers may be treating the token as a speculative instrument without an intention to participate in its future utility. There are often instances of futures trading for some tokens prior to their distribution under an ICO.

ICO as a distribution of securities (cont'd)

- **Functional differences to forms of non-securities crowdfunding.** Stakeholders argue that many businesses proposing ICOs use a coin or token in a manner similar to a prepayment of a good or service. However, regulators have observed that some ICOs issue coins or tokens that are readily tradable with an available secondary market, unlike the standard lack of transferability observed with prepaid promises to deliver under non-securities crowdfunding platforms such as Kickstarter.

- **Whether the utility function is available at the time the tokens are sold.** Most businesses that conduct ICOs are prospective and looking to raise capital to build out the utility function for the token. However, it has been argued that where some businesses have already built out the product for which the tokens are needed, the token may be less of a speculative instrument compared to a token whose utility function is not available at the time the token is sold.

- **Whether the business conducting the ICO has created an impression that the token is an investment or profit opportunity.** ICOs are conducted through the internet and can attract a wide range of potential buyers. Where a business is offering tokens and indicates that such token may generate positive returns for a buyer outside its use, the business may be creating the impression that such coin or token is actually an investment instead of a token with a specific use. This promotional aspect may be observed even where the business is separately asserting that the token is intended to be used for a utility function.

ICO models

- The most common ICO model is where a business raises capital by selling non-functional tokens and uses those proceeds to develop the functionalities it advertised for that token. The business issues the non-functional tokens immediately to purchasers following the ICO. The following are some other ICO models that have been proposed or used by businesses:

    a) an ICO structured so that one token is a security used for capital raising prior to the development of the platform, and a second, functional token is used for deployment once the platform is operational;

    b) an ICO where the developer delays release of the token to a later time; and

    c) an ICO in which the first step involves the purchasers and developer entering into an agreement for the right to a functional token, and then a second step involves fulfilment of the agreement by releasing the token when the platform/ecosystem is functional.

- Regardless of the model or structure selected, it is important to note that regulators will consider the substance of a transaction, and not simply its form.

Regulatory Approaches to Virtual Currencies

- Canadian financial regulators are monitoring and taking varying approaches to respond to the challenges posed by virtual currencies. We do not have a definitive statement from the Bank of Canada or the Office of the Superintendent of Financial Institutions (OSFI) (the federal regulator of Canadian banks), although both have highlighted the risks/challenges.
- A "virtual currency" could mean cryptocurrencies purported to function solely as a medium of exchange, without any added utility or purpose (for example, **Bitcoin**).
- Securities regulators have heard arguments that virtual currencies fail the investment contract test when they are "highly decentralized". For these virtual currencies, it is argued, there is no common enterprise, and no expectation of profit that relies on the significant efforts of others. In addition, stakeholders have identified the following additional factors that securities regulators should consider in determining when a virtual currency is not an investment contract, and therefore not a security:
  - **No central governance for the coin.** For example, Bitcoin has no entity or entities with authority to set rules applicable to the coin on an ongoing basis.
  - **Creation or distribution of coins not dependent on a central issuer.** For example, new coins could be created or distributed through mining, staking or other decentralized forms of coin creation/distribution.
  - **Transfer and trading of coins not dependent on a central party.** There are no restrictions on who may record new transactions on the blockchain ledger for the coin, and there is no central entity that can influence which transactions occur.
- As you can see, **it is far from obvious how to best classify a particular cryptocurrency**.

Key concern for ICO issuers and ICO investors: ***resale***

- For Canadian private issuers, unless specific relief is obtained, the securities coins/tokens issued under an ICO will be subject to a perpetual "hold period", namely holders will not be able to resell or trade their coins/tokens unless they are able to rely upon an existing statutory exemption from the prospectus requirement of applicable Canadian securities laws.
- As mentioned, it can be challenging to get discretionary relief if the structure does not fit within the precedent decisions
- Possible solutions?
  - Filing a prospectus (onerous and costly – issuer may not have team and protocols and the involvement of a licensed IIROC dealer is likely required)
  - Using an existing "reporting issuer" for a transaction (for example, a reverse takeover) and the issuance of the securities (not always practical or appropriate)
  - Creating a parallel continuous disclosure site for the token issuer where continuous disclosure documents (ie. financial statements, monthly updates as to the status of the project and the number of issued and outstanding securities tokens) are posted for consultation by existing and potential token holders and investors (similar to SEDAR in Canada or EDGAR in the US)

mcmillan

The Evolving Landscape of Cybersecurity Law in Canada: New Breach Notification Obligations and Guidance from the Regulators

Lyndsay A. Wasser, Partner, McMillan LLP

October 2, 2018

McMillan LLP

Vancouver
Calgary
Toronto
Ottawa
Montréal
Hong Kong

mcmillan.ca

Cybersecurity - Statutory Requirements to Protect Personal Information

- Privacy legislation throughout Canada requires protection of personal information (PI)
  - *Personal Information Protection and Electronic Documents Act* (PIPEDA) – PI must be protected by security safeguards appropriate to the sensitivity of the information; you must protect PI regardless of the format in which it is held; the nature of the safeguards depends on the format of the information; and the methods of protection should include technological measures (e.g., passwords and encryption).
  - Alberta & B.C. – Organizations must protect personal information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, modification, disposal or destruction.
  - Quebec – Enterprises must take the security measures necessary to ensure protection of PI, which are reasonable based upon sensitivity and the medium on which it is stored. Additional requirements under the *Act respecting the legal framework for information technology.*
  - Public sector legislation – Alberta, B.C., Manitoba, N.B., Nfld & Labrador, N.S., Ontario, P.E.I., Quebec, N.W.T., Nunavut, Yukon.
  - Health sector legislation – Alberta, Manitoba, N.B., Nfld & Labrador, N.S., Ontario, Saskatchewan.

Cybersecurity - Guidance from OPC Decisions

1. *Vtech Holdings Limited* – Deficiencies included:

- A lack of testing and maintenance to identify and mitigate vulnerabilities (the attacker exploited a well-known vulnerability to gain access to VTech's systems in this case). Vtech did not have a program of regular testing in place to identify such vulnerabilities.
- Inadequate administrative access controls – i.e., storage of production passwords in the test environment, sharing of accounts between staff, and local administrators having broad access across networks.
- Various cryptographic deficiencies – e.g., some information was stored in plaintext, some communications were transmitted in clear text, passwords were stored using cryptographic methods that were well-known to be vulnerable. Other information was stored in encrypted format, but keys were available within the compromised servers.
- Absence of security monitoring and logging to detect potential threats.
- No overarching comprehensive security management program.

Cybersecurity - Guidance from OPC Decisions

2. *Ashley Madison*

- Safeguards in place included:
  - Network segmentation, firewalls, and encryption on all web communications between ALM and its users, as well as on the channel through which credit card data was sent to ALM's third party payment processor.
  - All external access to the network was logged.
  - All network access was via VPN, requiring authorization on a per user basis; requiring authentication through a 'shared secret'.
  - Anti-malware and anti-virus software was installed.
  - Particularly sensitive information was encrypted, and internal access to that data was logged and monitored (including alerts on unusual access).
  - Passwords were hashed using the BCrypt algorithm (excluding some legacy passwords).

Cybersecurity - Guidance from OPC Decisions

Ashley Madison cont'd

- Deficiencies included:
  - Lack of multi-factor authentication (recommended industry practice)
  - Poor key and password management practices:
    - The VPN 'shared secret' was available on the ALM Google drive. Anyone with access to any ALM employee's drive on any computer, anywhere, could have potentially discovered the shared secret.
    - Instances of storage of passwords as plain, clearly identifiable text in emails and text files were also found on the systems.
    - Encryption keys were stored as plain, clearly identifiable text on ALM systems, potentially putting information encrypted using those keys at risk of unauthorized disclosure.
    - A server was found with an SSH key that was not password protected. This key would enable an attacker to connect to other servers without having to provide a password.
  - Lack of documented security policies or practices.

Cybersecurity - Guidance from OPC Decisions

3. TJX/Winners – Findings included:

- TJX had an encryption protocol in place (WEP), but it was weak.
- Experts had questioned the use of WEP as a secure protocol since 2003.
- TJX failed to convert to a stronger encryption standard within a reasonable period of time.
- TJX should have:
  - Segregated its data so that cardholder data could be held on a secure server while it undertook its conversion to WPA;
  - Adhered to PCI DSS version 1.1; and
  - Monitored systems vigorously for security threats.

Cybersecurity - Guidance from OPC Decisions

4. ***Peoples Trust*** – Findings included:

- The Company: "did not engage contractors with significant experience related to the design of financial services web applications, nor did it provide for minimum information security safeguard requirements in its contracts with such contractors."
- "As a result, customers' sensitive personal information: (i) was stored unnecessarily, in duplicate form and in perpetuity, on a vulnerable server in unencrypted format; and (ii) was accessed via a vulnerable web editor, which was maintained unnecessarily on the web server, even after it had been rendered obsolete."
- Peoples Trust also:
  - Failed to implement adequate monitoring and maintenance to ensure ongoing protection of personal information stored within its web server;
  - Had no program in place to install regular updates to the web editor; and
  - Lacked ongoing monitoring to detect potential security threats or weaknesses, and allow for proactive remediation before a breach occurred.

Cybersecurity - Guidance from OPC Decisions

5. WhatsApp – Findings included:

- Messages sent using the messaging system were not encrypted, and so there was a risk of interception, especially where a user elected to use the service through unprotected Wi-Fi networks.
- Even in cases where data was sent over ports used for secure https (SSL/TLS) communications, personal data (including the content of user messages and telephone numbers) was clearly visible.

6. CIBC – Concerns included:

- Lack of encryption; lack of supervision in data transfer; and apparent lack of technical accountability in data transfer.
- Windows platform used for the data transfers in question did not have an audit-trail capability to confirm the transmission of data to a portable disk drive.

Cybersecurity - Guidance from OPC Decisions

7. PIPEDA Report of Findings #2014-015 – Issues included:

- Outdated software, redundant systems containing personal information, insecure and inadequate logging, retention of data for longer than necessary, and a failure to isolate corporate computer systems from the engineering network.
- Password management was greatly hampered by the use of a deprecated encryption format and plain-text password hints – i.e. Plain text hints sometimes contained the password itself (or a very obvious hint) and the encryption format scrambled identical passwords in the same way.

8. *PIPEDA Report of Findings #2014-004* – The following safeguards were determined to be sufficient for compliance with PIPEDA:

- Firewalls; hashing and encryption of sensitive information; separate storage and obfuscation of encryption keys; and multiple intrusion detection systems.
- Safeguards independently evaluated on a regular basis through external vulnerability scans and an audit of its "at-rest" data protection practices against industry standards.
- A vulnerability management program was in place.

Cybersecurity - Mandatory breach reporting

- Mandatory breach reporting is becoming more common
  - Federal - PIPEDA (effective November 1, 2018).
  - Alberta – *Personal Information Protection Act.*
  - Newfoundland & Labrador – *Access to Information and Protection of Privacy Act.*
  - Saskatchewan – *The Freedom of Information and Protection of Privacy Act*; *The Local Authority Freedom of Information and Protection of Privacy Act.*
  - Northwest Territories & Nunavut – *Access to Information and Protection of Privacy Act.*
  - Health privacy legislation in Alberta, Newfoundland & Labrador, Nova Scotia, New Brunswick, Ontario, Prince Edward Island & Yukon.

Cybersecurity - Mandatory breach reporting

- **New PIPEDA requirements**
  - Organizations must report any breach of security safeguards involving personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.
  - Organizations must keep and maintain a record of ***every*** breach of security safeguards involving personal information under their control for 24 months, and such records must be provided to the Office of the Privacy Commissioner of Canada ("OPC") on request.
  - A breach of security safeguards is the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of the security safeguards required under PIPEDA or from a failure to establish those safeguards.

Cybersecurity - Mandatory breach reporting

- **New PIPEDA requirements, cont'd.**
  - The breach must be reported to the OPC.
  - Affected individuals must be notified of the breach.
  - The organization must also notify any other organization, government institution, or part of a government institution, if the other organization or government institution may be able to reduce or mitigate the risk of harm.
  - Every organization that knowingly contravenes the breach reporting or recording requirements is guilty of:

    (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or

    (b) an indictable offence and liable to a fine not exceeding $100,000.

Cybersecurity - Mandatory breach reporting

- **New PIPEDA requirements - What should you do now to prepare?**
  - ***Evaluation*** - What personal information do you process? Where/how is it collected, transmitted and stored? What safeguards do you have in place? Are they sufficient?
  - ***Remediation*** - Tighten controls. Train employees. Enforce policies.
  - ***Planning*** - Develop a comprehensive, customized breach response plan. Develop a record keeping system.
  - ***Testing*** - Security awareness testing. Test your breach response plan. Test your back-up systems.

Cybersecurity - Guidance from the Regulators

- **Guidance from the Privacy Regulators – A few examples:**
  - Guidelines for Identification and Authentication (OPC)
  - Tips for containing and reducing the risks of a privacy breach (OPC)
  - Privacy and Cyber Security. Emphasizing privacy protection in cyber security activities (OPC)
  - Securing Personal Information: A Self-Assessment Tool for Organizations (OPC) (Alberta OIPC & B.C. OIPC)
  - PIPA Advisory #8, Implementing Reasonable Safeguards (Alberta OIPC)
  - Mobile Devices: Tips for Security & Privacy (B.C. OIPC)
  - Responding to breaches – Each privacy commissioner has released guidelines

Cybersecurity - Guidance from the Regulators

- **Guidance from other Regulators**
  - ***Office of the Superintendent of Financial Institutions*** - Guideline B-10: Outsourcing of Business Activities, Functions and Processes; Cybersecurity Self-Assessment Guidance.
  - ***Mutual Fund Dealers Association of Canada*** - Bulletin #0690-C Cybersecurity; Bulletin #0744-C Electronic Communications Review.
  - ***Canadian Securities Administrators*** - Staff Notice 11-326 - "Cyber Security" (2013); Staff Notice 11-332 – "Cyber Security" (2016); Multilateral Staff Notice 51-347; CSA Staff Notice 11-336 – "Summary of CSA Roundtable on Response to Cyber Security Incidents.
  - ***Investment Industry Regulatory Organization of Canada*** - Cybersecurity Best Practices Guide; Cyber Incident Management Planning Guide; Administrative Notice – Dealer Member Cyber-security. See, also the Proposed Amendments [to Dealer Member Rules] Respecting Mandatory Reporting of Cybersecurity Incidents (April 2018).

Cybersecurity - Common themes in regulatory guidance

- An appropriate cybersecurity program requires:
  - Awareness of threats;
  - Self-assessment of vulnerability;
  - Implementation of a governance framework;
  - Training staff;
  - Following industry guidance and best practices;
  - Vulnerability and security testing;
  - Regularly reviewing controls;
  - Appropriate vendor selection and management, including appropriate contract terms; and
  - A breach response plan.

Cybersecurity - Other legal obligations and restrictions

- Statutes restricting certain activities:
  - Criminal Code – Using a device willfully to intercept a private communication; intercepting fraudulently and without colour of right any function of a computer system.
  - CASL – Provisions governing software installation, including provisions aimed at viruses and spyware.
  - *Radiocommunication Act* – Intercepting or interfering with radiocommunications; decoding encrypted subscription programming signal or encrypted network feed.
- Privacy torts & other civil claims (e.g., negligence, breach of contract)
- Do not forget contractual obligations!

Cybersecurity Landscape & Incident Response

Anne Feehely,
Associate General Counsel

BMO We're here to help.

LCCG Legal, Corporate & Compliance Group

Cybersecurity: An Overview

Cybersecurity Landscape| Privacy vs. Cybersecurity

vs.

Privacy

- refers to the laws that deal with the regulating, storing, and using of personally identifiable information of individuals, which can be collected by governments, public or private organizations, or other individuals.

Cybersecurity

- means a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

Cybersecurity Landscape| Compliance Frameworks

NIST (National Institute of Standards and Technology)

- US recognized framework consisting of standards, guidelines, and practices to promote the protection of critical infrastructure
- Cybersecurity Framework consists of three main components: the Core (a set of cybersecurity activities, desired outcomes, and references that are common across critical sectors), Implementation Tiers (provide how an organization views cybersecurity risk and how that risk is managed) and Profiles (represents the cybersecurity outcomes based on business needs)

ISO27000 (International Organization for Standardization)

- ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains
- Internationally recognized and covers the baseline security practices for stakeholders in the Cyberspace

COBIT (Control Objectives for Information and Related Technologies)

- Provides an internationally recognized framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT
- COBIT 5 incorporates globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems

Cybersecurity Legislation| Canada

PIPEDA

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is the Federal legislation that applies to the protection of employee personal information. It applies to federally-regulated organizations, and protection of personal information in the course of commercial activities in all jurisdictions in Canada that do not have similar legislation.

- Only three provinces currently have broad-based private sector privacy legislation in force: Alberta, British Columbia and Quebec.

Notification Requirements

PIPEDA requires organizations notify the Office of the Privacy Commissioner of Canada (OPC) if it is reasonable to believe that a breach of the security safeguards protecting personal information poses a "real risk of significant harm" to the affected individuals.

Mandatory breach notification has been part of Alberta's private sector privacy law since 2010 and becomes part of Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), on **November 1, 2018**.

Cybersecurity| Canada

Regulators

Office of the Superintendent of Financial Institutions (OSFI)

- Released the Cybersecurity Self-Assessment Guidance (2013) for FRFIs to assess their level of preparedness and to assist in the implementation of useful cybersecurity practice.

Investment Industry Regulatory Organization of Canada (IIROC)

- Released a Cybersecurity Best Practices Guide and a Cyber Incident Management Planning Guide (2015).

Canadian Standards Association (CSA)

- CSA emphasized the need for issuers, registrants and regulated entities to be aware of the challenges of cyber crime & take appropriate measures to safeguard themselves, clients or stakeholders under CSA Staff Notice 11-326/Staff Notice 11-332.

Notification Requirements

OSFI does not currently have in place regulations requiring specific actions by FRFIs with respect to cybersecurity. However, *Guideline B-10: Outsourcing of Business Activities, Functions and Processes* sets out OSFI's expectations with respect to cybersecurity risk management.

IIROC does not require mandatory reporting but is working to propose amendments to the Dealer Member Rules, requiring reporting. “As of now, IIROC advises that when a cyber-attack occurs that it be reported to IIROC promptly.”

Jurisdictional Challenges

Cybersecurity Landscape

Compliance Frameworks

NIST (National Institute of Standards and Technology)

- US recognized framework consisting of standards, guidelines, and practices to promote the protection of critical infrastructure
- Cybersecurity Framework consists of three main components: the Core (a set of cybersecurity activities, desired outcomes, and references that are common across critical sectors), Implementation Tiers (provide how an organization views cybersecurity risk and how that risk is managed) and Profiles (represents the cybersecurity outcomes based on business needs)

ISO27000 (International Organization for Standardization)

- ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains
- Internationally recognized and covers the baseline security practices for stakeholders in the Cyberspace

COBIT (Control Objectives for Information and Related Technologies)

- Provides an internationally recognized framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT
- COBIT 5 incorporates globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems

	Legislation	Regulators
	Personal Information Protection and Electronic Documents Act (PIPEDA)	The Office of the Superintendent of Financial Institutions (OSFI) Canadian Standards Association (CSA) Investment Industry Regulatory Organization of Canada (IIROC)
	Cybersecurity Information Sharing Act, 2015 (CISA) The Gramm-Leach-Bliley Act, 1999 (GLBA) California Consumer Privacy Act, 2018	NY Department of Financial Institutions (NYDFS) The US Securities & Exchange Commission (SEC) The Office of the Comptroller of the Currency (OCC)
	EU Data Protection Directive 95/46/EC	The General Data Protection Regulation (GDPR)
	Financial Conduct Authority (FCA)	Financial Conduct Authority (FCA)
	Personal Data Protection Act, 2012 (PDPA) Computer Misuse and Cybersecurity Act, 2017 (CMCA) Cybersecurity Act (not yet enacted)	Personal Data Protection Commission (PDPC) Monetary Authority of Singapore (MAS)
	No cybersecurity legislation	The Personal Data (Privacy) Ordinance (PDPO) The Office of the Privacy Commissioner for Personal Data (PCPD) The Securities and Futures Commission (SFC) The Hong Kong Monetary Authority (HKMA)
	The Cybersecurity Law of the PRC, 2017 (CSL) National Security Law, 2015 (NSL)	China Banking Regulatory Commission (CBRC)

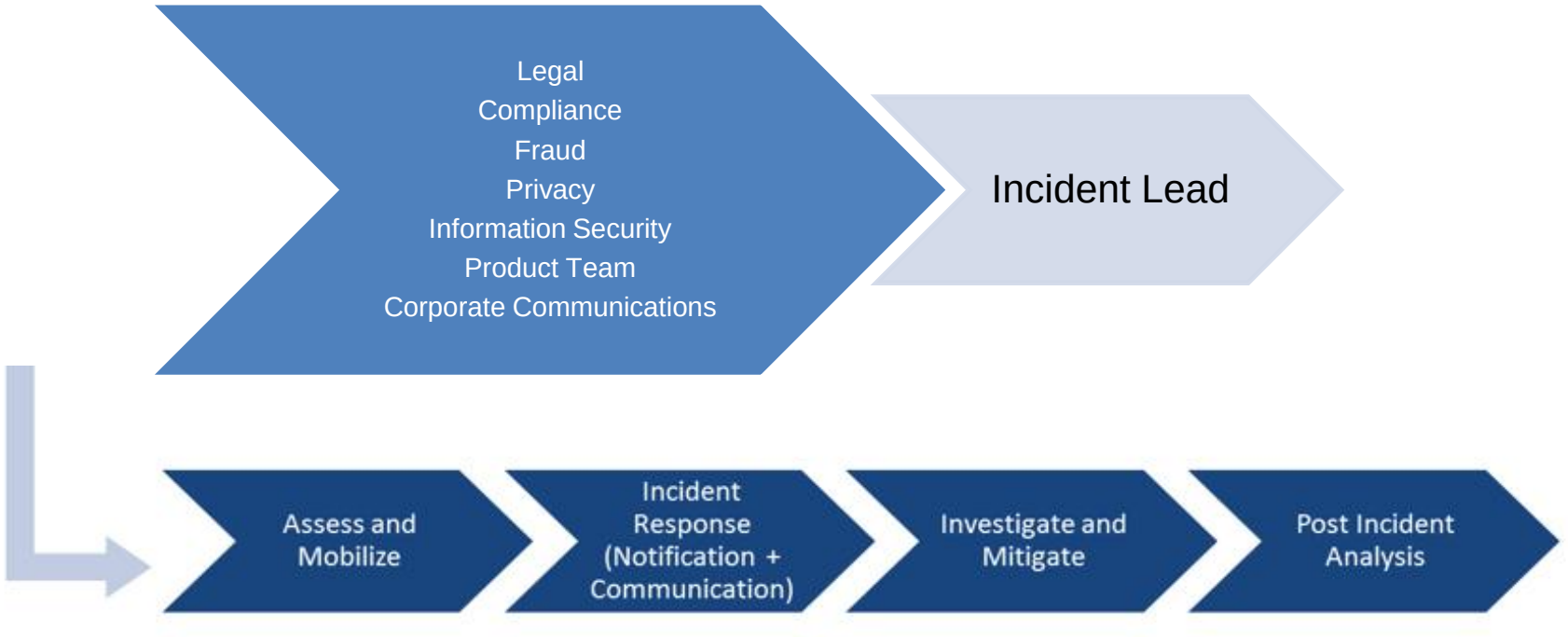
Cyber and Financial Institutions

- Cyber risks pose significant threats to BMO and other financial institutions
  - Reputational, financial, regulatory, customer and operational

- Risks are managed through different areas and levers. All have an important role to play:
  - Governance and controls
  - Product / Business teams
  - Cybersecurity Program (Information Security)
  - Third-party risk management system
  - Corporate support areas including Legal and Compliance

- What is an Incident?
  - An incident is a threat to the integrity and security of sensitive data

Incident Response Team



Ten Tips for Incident Response

1. Develop and Implement an Incident Response Plan
2. Create an Incident Response Team
3. Have a Lead Person
4. Determine which regulators must be notified
5. Build an Effective and Safe Workforce
6. Be Careful About What You Say In Your Company Privacy Policy
7. Make Continuing Education a Practice
8. Identify Outside Entities that will be Retained if an Intrusion is Discovered
9. Consider Cyber Insurance
10. Continually improve "Operational Security"

mcmillan

ACC Association of Corporate Counsel ONTARIO

Cybersecurity, Blockchain and Cryptocurrencies – Where Law and Technology Intersect

October 2, 2018

McMillan LLP

Vancouver
Calgary
Toronto
Ottawa
Montréal
Hong Kong

mcmillan.ca