Federation of Law Societies of Canada

Fédération des ordres professionnels de juristes du Canada

MEMORANDUM

FROM: CIV Subgroup – FLSC AML Working Group

TO: FLSC AML Working Group

DATE: April 24, 2019

SUBJECT: Report on CIV Issues Review

This memorandum reports on a number of issues reviewed by the CIV subgroup ("the subgroup") as follows:

1. Indian bands as public bodies
2. The definition of electronic funds transfer in the Model Rule
3. The definition of reporting issuer in the Model Rule
4. Issues relating to cryptocurrency
5. Issues relating to politically exposed persons ("PEPs")

1, Indian Bands as Public Bodies

While this issue was earmarked for review by Frederica and Leah, the subgroup decided that it would assist in supporting that review.

The subgroup reviewed earlier research completed by Jim Varro at a time when including or not including Indian bands in the definition of "public body" in the Model Rule was a live issue. Including Indian bands in the definition would mean that a lawyer would not be required to verify identity of this organizational client. The matter was not pursued at that time given the imminent revived litigation and concerns that the federal regime did not provide for Indian bands as exempt from the regulations as public bodies.

The subgroup noted a provision in the Income Tax Act ("ITA") that may be relevant to the issue. The following excerpt from a 2016 ruling from the ITA Rulings Directorate to the Charities Directorate deals with whether Aboriginal bands should be viewed as qualified donees for charity purposes. The CRA ITR Directorate concluded that all bands created under the *Indian Act* meet the criteria to be considered municipal or public bodies performing a function of government in Canada for the purpose of paragraph 149(1)(c) of the Act and exempt from income tax. Some 345 Indian bands/groups were included as qualified donees.

> July 27, 2016
> …
> In 1948, the Act was amended to include a tax exemption for "a municipality or a municipal or public body performing a function of

government". It appears likely that municipalities were considered part of the provincial Crown and were added to the list of tax exempt entities to make it explicit that they are not subject to income tax. There is no definition of "a municipal or public body performing a function of government" in the Act. However, it would seem logical, based on the wording, that it would appear to be an entity that is similar in nature to a municipality and governs people in a particular area.

The federal government, through the Indian Act, specifically creates an Indian band. Under the Indian Act, these bands or First Nations may be able to levy property taxes and create by-laws that affect its members. Consequently, **the very nature of an Indian band and its council under the Indian Act is that of a local government, similar in nature to a municipality.** This means that their reserve lands, monies, other resources and governance structure are managed by the provisions in the Indian Act. When a band council makes a by-law under this section, it must be explicitly approved by the Minister of Indigenous and Northern Affairs Canada.

In 2014 the Rulings Directorate instituted a service called Public Body Rulings as a pilot project. During this period Rulings has gathered even more extensive experience with determining whether a band qualifies as a municipal or public body performing a function of government in Canada. As a result, **it is our view that all bands created under the Indian Act meet the criteria to be considered municipal or public bodies performing a function of government in Canada** for the purpose of paragraph 149(1)(c) of the Act and are therefore exempt from income tax.

If you have any questions with respect to this policy please do not hesitate to contact me. We trust that our comments will be of assistance.

Roger Filion, CPA, CMA
Manager
Non-Profit Organizations and Aboriginal Issues
Business and Employment Division
Income Tax Rulings Directorate
Legislative Policy and Regulatory Affairs Branch

(emphasis added)

While the ruling only applies in the context of the ITA for the purpose of taxation, there is an argument that this conclusion could be extended to determine that Indian bands are like municipalities and thus should be included in the definition of "public body" in the Model Rule.

Proposal: The sub-group's suggested approach is that the Working Group assess this and determine the merits of the position. If there is agreement that this be explored as an amendment to the Model Rule, it is suggested that it may be appropriate to flag this for informal discussion with the Department of Finance at the appropriate time to explore how they might view the FLSC proposal to consider Indian bands as public bodies.

2. The definition of electronic funds transfer ("EFT") in the Model Rule

Based on some feedback received during the call for comment on the Model Rule amendments and concerns expressed by some law societies, the sub-group reviewed the exemption from the verification requirements if funds are transferred via EFT. The primary questions were whether anyone really used the exemption and whether the exemption is appropriate given the understanding that transfers of funds by this method were common.

This prompted a review of the definition of EFT in the Model Rule. Based on research conducted by sub-group members, this is what was learned:

- EFTs include a variety of methods of funds transfers, including on-line banking transactions, direct debit transactions, credit card transactions and electronic bill payments
- EFT is the process of transferring funds electronically
- Wire transfers are one form of EFT and involve transferring funds from one account to another – it is a bank to bank transaction
- The definition in the Model Rule is essentially a definition for wire transfers

Through Anthony, we obtained information from a lawyer in a senior role working in the AML department of one of the big 5 banks who commented on our definition as follows:

- This level of detail would be required for LVTS/Wire transfers and International remittances – it generally would not apply to domestic transfers or e-transfers
- Although the level of detail set out in definition may not be on the record of the client, the bank would, in some cases, be able to get this level of detail for other products; the due diligence conducted by the bank in these matters would depend on the frequency of use of the method of payment and the nature of the business the account is set up for
- Bank generally screens the account holder when they open the account, and may do additional risk assessment if client asks to use these methods to move funds (one-off versus ongoing use of these methods).
- They may enquire about the purpose of the transaction source of funds etc. – this would not generally occur if the money is being moved from a law firm's trust account, as the law firm/client would generally claim privilege about the transaction and could refuse to provide details
- The bank is only scrutinizing the client, either the sender or the recipient. If it is the law firm that is sending/receiving, they will not be doing any scrutiny of the client of the law firm behind the transaction
- What if your bank is on the receiving end of this transfer, and the name does not match the account number. In 99% of the cases it would match, possible that if it did not, it could be rejected.

Literature published by the Royal Bank indicates that to send a wire, the bank requires the full name, address and account number of the sender and the recipient.

We also communicated with a senior partner at a large national law firm who is an expert in AML and banking law. This lawyer was also part of the group that helped the FLSC frame the definition of EFT for the model rule when the CIV rule was being drafted. She advised that the large firms use the exemption all the time. As it defines wire transfers, the full extent of the "know your client" requirements applicable to the banks are applied in these transactions for the account holders who are sending and receiving the funds.

She advised that most financial institutions will require that the lawyer, if instructing a wire transfer, to disclose any third party on whose behalf the wire is instructed. She also said that this will become a requirement under the new regulations (which she anticipated would be in force within the year) when a person instructs a bank to do a wire transfer that is over $10,000.

Proposal:

While acknowledging the input received and the issues discussed above, a majority of the sub-group members believe that the EFT exemption should be reconsidered; some within that majority believe it should be removed. In summary, the concerns are:

- The potential for misuse of the exemption, thereby creating a risk that money laundering may occur
- A sense that the exemption is not understood
- A sense that the exemption is not used, which raises a question as to its value
- Not understanding the situations in which the exemption would in fact be used

The sub-group discussed whether further research on the application of the exemption would be appropriate, including obtaining information from firms that have used the exemption on how it is applied. While this idea wasn't dismissed, at present the subgroup thought that a discussion in the larger working group would be appropriate first to determine next steps in addressing this issue.

3. The definition of reporting issuer in the Model Rule

The following is background to this issue.

When the CIV Model Rule was being drafted, an exemption from the ID verification requirements for corporate entities, similar to that in the federal regulations, was included. The federal regulations say that the requirements for record-keeping and ascertaining identity do not apply where the entity is a corporation that has minimum net assets of $75 million on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange designed under subsection 2652(1) of the *Income Tax Act*, and operates in a country that is a member of the Financial Action Task Force (FATF).

As you know, our exemption does not specify corporations but a 'reporting issuer'. The definition of 'reporting issuer' uses very similar language to the regulations[1] but also captures entities that may not be corporations such as real estate investment trusts (REITs). In looking back on how this definition was adopted, the following is an excerpt from a November 2008 memo documenting discussion with the group of large firms reps the LSO convened to assist in the technical aspects of the CIV rule:

[1] "reporting issuer" means an organization that is a reporting issuer within the meaning of the securities laws of any province or territory of Canada, or a corporation whose shares are traded on a stock exchange that is designated under section 262 of the Income Tax Act (Canada) and operates in a country that is a member of the Financial Action Task Force, and includes a subsidiary of that organization or corporation whose financial statements are consolidated with those of the organization or corporation.

- …the term "corporation" is antiquated in terms of the publicly-traded entity – includes more that corporations or companies

- Language should capture idea of the public issuer as defined in securities legislation, whether a corporate structure, a trust, etc.; this would include REITS and other publicly traded income trusts, publicly traded limited partnerships, etc.

- Language should be flexible enough to accommodate changes that may occur in the securities law definition of "public issuer"

- Suggested draft language, which is to be refined with further input from the reps, is as follows:

  > "reporting issuer" – an organization that is a reporting issuer as defined in securities legislation in any province or territory of Canada or the equivalent of a reporting issuer in a country that is a member of or has observer status with the Financial Action Task Force

  (subsidiary whose financial statements are consolidated, etc. to be included as well)

Presently, concerns were expressed about whether the definition of 'reporting issuer' should be maintained. This arose because there was a sense that the regulation of reporting entities in other countries may not be as robust as in Canada and there may be risks in simply accepting that because they are regulated in some fashion, they need not be subject to verification requirements.

In speaking with the expert referred to above about this issue, she advised that the definition in referencing Canadian jurisdictions' securities regulation, the applicable section of the Income Task Act (ITA) and the FATF countries ensures there is robust regulation. In particular, she advised that the s. 262 ITA provision imposes a rigorous standard and regulatory scrutiny. In her view, especially since the definition imports language from the federal regulations, this definition does not create a risk. As a final point, she mentioned that industry has been pressing the federal government for some time to change the exemption in the federal regulations to look more like our definition, given that, currently, entities such as REITs are not included in the exemption.

Proposal:

At least one member of the sub-group determined that this issue required further thought. As such, no consensus was reached on whether the information obtained noted above is satisfactory, to the extent that the sub-group could determine that it had no concerns about use of the definition. Similar to the issue around the EFT exemption, the sub-group is suggesting that this matter be discussed in the larger group and a determination made on next steps, based on the information provided here.

4. Issues relating to cryptocurrency

Sub-group members Anthony and Susan prepared a memo on the risks of cryptocurrency for the legal profession, **attached**. The memo provides a good summary of the subject and sets out some important considerations for the legal profession. Also **attached** is a scan by the FLSC Trust Assurance Group on some law societies' treatment of cryptocurrency.

We are aware that the Department of Finance has begun to consider cryptocurrencies in the context of its AML regime, and it is contemplated that this may form part of discussions among the FLSC and Finance reps in their engagement.

Proposal: It is suggested that the memo be considered and discussed by the Working Group. It may be that this issue is appropriate for referral to other FLSC groups, such as the trust administrators of the Model Code committee, for review. Developments at the federal level should continue to be monitored.

5. Issues relating to politically exposed persons ("PEPs")

Sub-group members Chioma and Jeanette prepared a research memo on PEPs, **attached**, which includes a list of considerations related to PEPs, legal professionals obligations and some key questions.

The Department of Finance has indicated that the list of reporting entities required to deal with PEPs is proposed to be expanded in future regulations. They are aware that our review of PEPs in the context of the Model Rule obligations was part of the Working Group's phase II review.

Proposal: It is suggested that the memo be considered and discussed by the Working Group, and determination made as to how, if at all, PEPs should be incorporated into the current obligations under the Model Rule.

RISKS OF CRYPTOCURRENCY FOR LEGAL PROFESSION

INTRO:

What is "Cryptocurrency"?

Cryptocurrencies are a type of digital currency created using computer algorithms. The most popular cryptocurrency is Bitcoin[1]. Bitcoin is not the only cryptocurrency...there are at least 2000 other types. These virtual currencies are here to stay and have value, although extremely volatile.

No single organization, such as a central bank, creates digital currencies. Digital currencies are based on a decentralized, peer-to-peer (P2P) network. The "peers" in this network are the people that take part in digital currency transactions, and their computers make up the network. Cryptocurrencies are traded on dozens of various digital currency exchanges throughout the world.

Using digital currencies

Digital currencies can be used to buy goods and services on the Internet and in stores that accept digital currency. They may also be bought and sold on open exchanges, which is similar to a stock market and called digital currency or cryptocurrency exchanges.

To use digital currencies, users need to create a "digital currency wallet" to store and transfer digital currencies. Users can store their wallet themselves or have a wallet provider manage their digital currency for them.

Users need a "public key" and a "private key" to use their wallet. These keys are made up of a random sequence of numbers and letters.

Public keys are used to identify a user's wallet.

Private keys are used to unlock a user's wallet and access their money. Private keys should be kept secret.

All transactions are recorded to a public ledger or "blockchain" that everyone can see.

Digital currencies are not a legal tender

Digital currencies, such as Bitcoin or other cryptocurrencies, are not legal tender in Canada. Only the Canadian dollar is considered official currency in Canada.

The *Currency Act* defines legal tender as:

- Bank notes issued by the Bank of Canada under the Bank of *Canada Act*; and
- coins issued under the *Royal Canadian Mint Act*.

Digital currencies are not supported by any government or central authority, such as the Bank of Canada.

Financial institutions, such as banks or credit unions, don't manage or oversee digital currency.

---

[1] **CRA:** https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html

Tax rules apply to digital currency transactions, including those made with cryptocurrencies. Using digital currency does not exempt consumers from Canadian tax obligations.

This means digital currencies are subject to the *Income Tax Act*.

Buying goods or services using digital currency – Tax issues

Goods purchased using digital currency must be included in the seller's income for tax purposes. GST/HST also applies on the fair market value of any goods or services purchased using digital currency.

Buying and selling digital currency like a commodity

Any gains or losses from selling or buying digital currencies must be reported when taxes are filed.

Digital currencies are considered a commodity and are subject to the barter rules of the *Income Tax Act*. Not reporting income from such transactions is illegal.

Learn more about the Canada Revenue Agency's reporting requirements for digital currencies.

GENERAL RISKS OF USING DIGITAL CURRENCY

Exposure to fraud

Digital currencies may be vulnerable to fraud, theft and hackers.

All transactions are recorded to a public ledger or "blockchain". The blockchain may include information such as transaction amounts, wallet addresses and the public keys of the sender and recipient. Users are pseudonymous – that is, they can send and receive cryptocurrency without providing personally identifying information. The level of anonymity provided may attract cybercriminals to move or steal funds, or make donations to illicit groups.

Since it's founding, digital currency has developed a reputation for assisting criminal activity, including money laundering, tax evasion, child pornography, the drug trade and for being the go-to currency for other online illegal good.

Fewer protections

Cryptocurrencies are not backed by governments or financial institutions, which creates uncertainty to their reliability, value and traceability, as well as their legal status.

Access to a complaint-handling process as available with other payment methods, such as debit and credit cards, is limited.

Even if a wallet provider is used to help manage digital currency, the provider does not have to help get funds back if something goes wrong with the transaction.

Deposits are not insured

It's the users' responsibility to protect their digital currency wallet.

Federal or provincial deposit insurance plans don't cover digital currency. For example, the Canada Deposit Insurance Corporation (CDIC) only covers eligible deposits in Canadian dollars at member financial institutions if the institution fails.

If the currency exchange or wallet provider that has the users' digital currency fails or goes bankrupt, their funds won't be protected.

Investments may be high risk

Digital currencies can be risky investments because their value can increase or decrease over a very short period of time. Such changes in value can be difficult to predict. Digital currency may be worth less than it was when purchased.

You may have a hard time exchanging your digital currency

Digital currencies can be difficult to buy and use, and may not be easily exchanged for cash or accepted by merchants to purchase goods and services.

Transactions are not reversible

Purchases and transactions made with digital currencies are not reversible.

This means:

- users can't reverse the charges if the product was not received;
- users can't get their money back unless the seller agrees; and
- users might not be able to stop a payment.

CONSIDERATIONS FOR THE LEGAL PROFESSION:

- Lawyers must maintain a high level of awareness of the potential red flags listed above should a client wish to transact in cryptocurrency.
- Risk assessments by lawyers must involve an analysis of potential threats and vulnerabilities to money laundering and terrorist financing crimes.
- Authorities will be vigilant of legal professionals advising clients and helping clients to transact using digital currencies.
- Lawyers need to determine exactly what their clients want to do; therefore it's important to ask their clients the right questions.
- Implement "know-your-client" procedures and identify any third-party payors prior to acceptance of payments made with digital currency.

- Because digital currency is property rather than actual currency, it cannot be deposited into a client trust account; therefore, other methods of storage will be required. For instance, if it is treated as "valuable property", then documents will need to be maintained to track receipt of the digital currency and it must be kept safe.
- Despite digital currency's reputation for high-level security; the potential for hacking and theft from exchanges is one of the biggest threats to the security of the transactions and poses a significant risk of loss should such events occur.
- Because digital currencies aren't regulated and are anonymous, they are speculative and extremely volatile. Price fluctuations are considered to be one of the biggest risks to the future success of digital currencies, with many influencing factors including increased regulatory scrutiny, which if gets too stifling, could send the value of digital currencies plummeting.

Some Helpful Advice from the *Nebraska Ethics Advisor Opinion for Lawyers*, No. 17-03:
(https://supremecourt.nebraska.gov/sites/default/files/ethics-opinions/Lawyer/17-03.pdf)

Fees for Legal Services

- The opinion states that lawyers may accept payments in digital currencies, but must immediately convert them into U.S. dollars. Any refund of monies is also made in U.S. dollars and not in digital currency.
- As the value of digital currencies often fluctuate dramatically, an arrangement for payment for legal services in digital currency could mean that the client pays $200/hour in one month and $500/hour the next month, which the client could very easily allege as unreasonable or unconscionable. Conversely, if the market value of the digital currency used as payment quickly fell, the lawyer would be underpaid for services.
- To mitigate or eliminate the risk of volatility, it is possible to value or convert digital currency into cash immediately upon receipt. In this way, the client's account would be credited appropriately and there would be no risk to the client of value fluctuation. As part of this process, a law office would need to notify the client that the firm would not be retaining the digital currency, but converting it to cash upon receipt. Through this method, the client is informed that an increase in the value of their digital currency will not additionally fund their outstanding account. In addition, clients need not be concerned if the value of the digital currency they sent for payment suddenly dropped.
- Including this information in the fee agreement between lawyer and client is probably one of the best ways to ensure the client is property informed.

.

Identification

- The dilemma faced in identifying a third-party payor is that the use of digital currencies is pseudonymous and often close to anonymous. Sufficient information needs to be requested from the third-party payors prior to the acceptance of the digital currency payment.

Security

- Due to security concerns, the lawyer must take reasonable security precautions as there is no bank or insurance coverage to reimburse a digital currency holder if a hacker steals them. Once lost, digital currency could be gone forever. Reasonable methods could include encryption of the private key required to send the digital currency. Another method may include utilization of more than one private key. Other reasonable measures may include maintenance of the wallet in a computer or other storage device that is disconnected from the Internet (also known as "cold storage"), a method that would also allow for off-line storage of one or more private keys.

OTHER CONSIDERATIONS

- Lawyers are required to safeguard client property. This means they must ensure their digital "wallet" is secure and backed up. The provider of the wallet is not responsible for the safekeeping of the wallet or if anything goes wrong with the transaction.

- Law Societies' regulation of trust accounts and recordkeeping has not kept pace with technology and does not contemplate digital currency. For the most part, regulators are also currently not equipped to audit digital currency transactions and storage.

FLSC Trust Assurance Group
Environmental scan pertaining to the acceptance of cryptocurrencies – April 2019

Jurisdiction	Process
Notaires du Québec	• Notaires du Québec Trust accounting By-law authorizes the notary to hold goods and sums without any specification in regards to the kind of goods. In that respect, cryptocurrencies are considered as "goods". • No transaction by a notary with cryptocurrencies as been declared yet. However, the Chambre des notaires is concerned about the way the notary would ensure that the goods is client's property and how the notary could hold the goods (holding the bitcoin key, password, etc).
Ontario	• Bitcoin cannot be used as a monetary retainer as it cannot be accepted into a trust account and a licensee would not be able to comply with their trust accounting obligations • Bitcoin can be used as payment for fees – once services are rendered and billed. We see this as no different than any other form of barter • Advanced agreement to pay fees in Bitcoin may be problematic – it may not meet the “fair and reasonable” requirement for fees – it would be preferable to value the services in Cdn currency and then to accept the equivalent payment in Bitcoin • Some risks that would apply to any business that transacted in cryptocurrencies - volatility of exchange/value; access and security over wallet; anonymity of users (lawyer would have to comply with record keeping bylaws on documenting the transaction); then there is the question of AML implications of transacting in cryptocurrencies; tax implications of gains/losses on holding cryptocurrencies (especially impacted by its volatility). These are some of the perceived business risks.
Alberta	• There is nothing in our rules that restricts how a lawyer is reimbursed for legal services provided to a client that have been completed and properly billed. • Money received by a layer in trust for a client must be deposited into a chartered bank, provincial savings office, credit union or a league to which the Credit Unions and Caisses Populaires Act, 1994 applies, or a registered trust corporation. It is our understanding that cryptocurrencies cannot, at this time, be deposited into an account at any of these financial institutions although that doesn’t necessarily preclude a firm from accepting the cryptocurrency, selling it on the exchange and depositing the proceeds in a bank. • Not permitted into Trust. Rules are silent on acceptance into General Account or receipt as trust property
BC	• Not permitted into Trust. Rules are silent on acceptance into General Account or receipt as trust property

Memo

To: FLSC AML WORKING GROUP PHASE II

From: Chioma Ufodike and Jeanette McPhee

Date: January 18, 2019

Re: Research on Politically Exposed Person (PEP) And the Head of an International Organization (HIO)

---

1. INTRODUCTION

A politically exposed person (PEP) or the head of an international organization (HIO) is defined by FINTRAC is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO has puts them in a position to impact policy decisions, institutions and rules of procedure in the allocation of resources and finances, which can make them vulnerable to corruption[1].

Due to their position and influence, the Financial Action Task Force (FATF) recognizes that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF)[2]. FATF recommends that all countries consider domestic as well as foreign politically exposed persons and heads of international organizations as part of the approach to combatting money laundering and the financing of terrorist activities[1].

2. DEFINITIONS

a. ***Foreign PEPs***[3]: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
b. ***Domestic PEPs***[4]: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

---

[1] http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide12/12-eng.asp

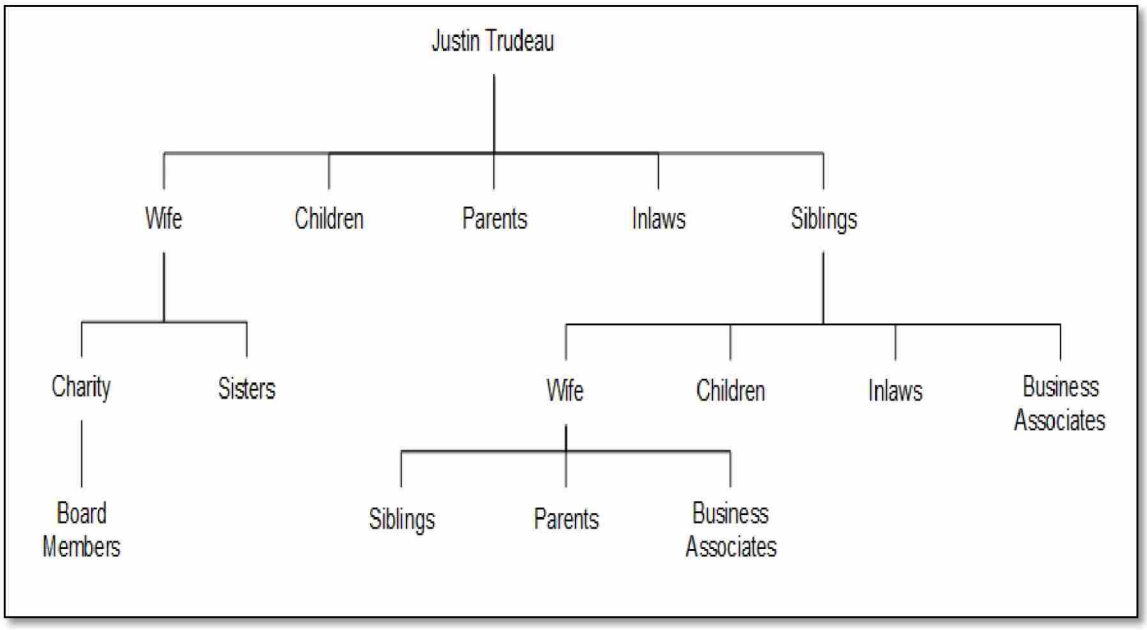
[2] June 2013 FATF Guidance: Politically Exposed Persons http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

[3] Example: head of state or government, member of the executive council or legislature, deputy minister, ambassador, judge of supreme court, leader or president of a political party etc. A person determined to be a foreign PEP, is forever a foreign PEP

[4] Example: deputy minister, head of government, ambassador, president of a corporation that is wholly owned by her majesty, mayor, leader of political party etc. A person ceases to be a domestic PEP 5 years after they have left office

c. ***International organization PEPs***[5]: persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. President, CEO, directors, deputy directors and members of the board or equivalent functions.
d. ***Family members***[6]: individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.
e. ***Close associates***[7]: individuals who are closely connected to a PEP, either socially or professionally.

Figure 1.1 Sample PEP Law Regime



Source: Christine Duhaime, BA, JD, CAMS Presentation to AML Working Group Toronto June 1, 2017

3. FINTRAC OBLIGATIONS TO DETERMINE PEP STATUS

The reporting entity sectors with the obligation to determine whether a person is a foreign PEP, a domestic PEP, a HIO, or a family member of close associate of one of these people, are financial entities, securities dealers, money services businesses and life insurance companies. Other reporting entities, such as the British Columbia

[5] Example: The president or CEO of international Energy Agency, Common Wealth, Bank for international settlements, NATO etc Once a person is no longer the head of an international organization or the head of an institution established by an international organization, that person is no longer a HIO
[6] Example: spouse or common-law partner, their child, their mother and father, mother or father of their spouse or common-law partner and child of their mother or father (sibling)
[7] Example: business partners, charity, board member, same political party, romantic relationship etc

notaries, the real estate sector and the accounting sector, are not obligated to determine PEP status.[8]

4. WHEN TO MAKE A PEP DETERMINATION

Part of knowing your clients is determining whether a person is a foreign PEP, a domestic PEP, a HIO, or a family member or close associate of one of these people[9].

There are five instances that will trigger PEP and HIO obligations:

- on account opening
- on a periodic basis for existing account holders
- if you detect a fact about an existing account holder
- when you conduct an incoming or outgoing electronic funds transfers (EFT) of $100,000 or more
- a person makes a lump-sum payment of $100,000 or more towards an immediate or deferred annuity or life insurance policy

a. Foreign PEP: They must take reasonable measures to determine whether a person is a foreign PEP, or a family member or close associate of a foreign PEP. Foreign PEPs, their family members and their close associates must automatically be treated as high-risk clients.
b. Domestic PEP: They must take reasonable measures to determine whether a person is a domestic PEP or HIO or is a family member of a domestic PEP or HIO. Once they determine that a person is a domestic PEP, a HIO, or the family member or close associate of a domestic PEP or HIO, they must assess to determine if that person poses a high risk for committing a money laundering or a terrorist activity financing offence. If they assess the risk to be high, then the person must be treated as a high-risk client.

When these obligations came into force (June 17, 2017), Fintrac did not require the reporting entities to assess all of their existing account holders immediately, but expected that, within their policies and procedures, there would be a process by which existing account holders would be assessed over time, and in line with their obligation to take reasonable measures on a periodic basis[1].

5. HOW TO MAKE A PEP DETERMINATION

The PCMLTFA requires that reporting entities take "reasonable measures" to make the PEP determination. Reasonable measures could include:

- Asking the individual for information that could indicate PEP status, such as existing or previous connections to the prescribed relationships;

---

[8] http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/1-eng.asp

[9] The reporting entities with these obligations include financial entities, securities dealers, money services businesses and life insurance companies.

- Screening the individual's name and other personal information against a commercially or publicly available database to gather more information about the individual; or
- a combination of both[10].

If they have already determined that a person is a foreign PEP or the family member of a foreign PEP, they are not required to make this determination again.

In addition, the reporting entities must take reasonable measures to establish the source of funds for any account or EFT's or lump sum payment, of $100,000 or more.

Reporting entities must keep PEP and HIO records for at least five years from the date the account to which they relate is closed.

The regulations also require that reporting entities must keep a record if the reasonable measure was unsuccessful, and they were unable to make a conclusive determination[1].

6. WHAT HAPPENS AFTER A PEP DETERMINATION IS MADE

For high-risk PEPs, HIOs, their family members and close associates, reporting entities have specific obligations to keep records, establish source of funds, obtain senior management review of a transaction, or approval to keep the account open and conduct enhanced ongoing monitoring of the PEP's account.

7. LEGISLATIVE AND REGULATORY GAPS

Section 9.3 of the PCMLTFA requires all reporting entities to determine whether it is dealing with a PEP, a prescribed family member of a PEP or an individual who the person or entity knows or should reasonably know is closely associated – for personal or business reasons – with a PEP.

The Department of Finance published a discussion paper entitled Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime (the Discussion Paper) in February 2018. This report identified a number of legislative and regulatory gaps in the regime and provided suggestions with respect to politically exposed persons (PEP).

Recommendation #2 states that:

The Government of Canada should review, refine, and clarify through training, the statutory definition of politically exposed persons (PEP). In particular, the notion of 'association with a PEP' under this definition creates ambiguity and inconsistency among institutions in regard to who exactly constitutes a PEP[11].

Recommendation #3 states that:

The Government of Canada move to a risk-based model of compliance for politically exposed persons, softening the requirements for those with transparent and unsuspicious financial portfolios[11].

---

[10] OSFI Deterring and Detecting Money Laundering and Terrorist Financing, December 2008 http://www.osfi-bsif.gc.ca/Eng/Docs/b8.pdf

[11] Confronting Money Laundering and Terrorist Financing: Moving Canada forward. Report of the Standing Committee on Finance November 2018

These two recommendations from the Discussion Paper follows discussion at the Standing Committee on Finance in 2018 that there should be a reliable method of identifying PEPs, such as a registry, in place, to allow reporting entities to be able to comply with the PEP requirements[11]. It was pointed out that the identification of PEPs is troublingly inconsistent as reporting entities determine the extent to which they apply due diligence procedures to PEP identification, and that the definition of a PEP under Canadian law is overly broad. Larger financial institutions will subscribe to media advisory services but smaller reporting entities do not have the capacity to operate or subscribe to these services. It was argued that a central registry or database of PEPs in Canada would address these problems with the AML/ATF regime[11].

The practical issue remains that there is no clear way to designate and identify PEPs due to the lack of available and useful information about the identity of PEPs around the world. There are private providers of PEP databases, however the information contained in them and the ability to positively match the client with a PEP in a database can be challenging. In addition, there is a cost to this service which could be significant to law firms. Also, PEPs are becoming more creative in finding ways to avoid detection, such as opening accounts in the names of corporations instead of their own names, so the PEP lists may not be effective. Using name checking lists is not easy as many PEPs may have numerous "Also known as" alternative names. Also, naming customs and protocols from other countries are not always understood, many names are the same, and there are not unique identifiers, such as address or date of birth[12].

Similar issues may occur when using name checking lists that apply to Canada's legislative measures against terrorists, terrorist groups and other listed and sanctioned individuals and entities ("Designated Persons") are contained in various Canadian statutes and regulations, which apply to all Canadians through various Canadian statutes and regulations, including federally regulated financial institutions[13].

8. PROPOSED REGULATORY AMENDMENTS

In 2015–16, the FATF evaluated Canada's AML/ATF Regime, and identified a number of deficiencies. The proposed regulatory changes address a number of the deficiencies outlined by the FATF.

Specifically, the proposed amendments clarify existing requirements relating to the source of wealth of politically exposed persons:

"*An amendment to require reporting entities to take reasonable measures to determine the sources of a politically exposed person's wealth. The amount of a client's accumulated funds or wealth should appear to be reasonable and consistent with the information provided, and doubts about the origin of such funds or wealth would have to be satisfied before a reporting entity proceeds with the relationship or permits transactions to occur*"[14].

[12] CAMS Certification Examination Study Guide, ACAMS, 2012
[13] http://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/Pages/dsninstr.aspx
[14] Canada Gazette Part I Saturday June 9,2018 : http://gazette.gc.ca/rp-pr/p1/2018/2018-06-09/pdf/g1-15223.pdf

The final version of the amendments was published in the fall of 2018, with implementation 12 months later, in the fall of 2019.

9. FURTHER CONSIDERATION

The Federation AMLTF Working Group will need to consider whether PEP & HIO identification should be included in the Model Rules, how that might be done, and if so, what we should consider if we decide to include PEP & HIO requirements.

This raises a number of issues to consider:

- Other service providers are not obligated to do this. Will the Federal regulations for other service providers be changed in the future? Should we mirror the Federal regulations, or go beyond?

- Should PEP & HIO be mandatory, recommended or not recommended? Should it be must or reasonable measures?

- As the information is difficult to obtain, or inconsistently obtained by reporting entities, what will be our requirements? How will lawyers determine which clients are higher risk, to obtain PEP & HIO information from?

- If it is recommended, what will be the cost of obtaining this information for lawyers, as it is not readily available? Who will pay for this?

- If our position is to recommend PEP and HIO identification:
    - What risk-management systems will be used to determine whether the client is a PEP? There is no central database so should they subscribe to a third party database (e.g. WorldCompliance® screening database) which increases compliance costs for firms. In addition when do you check? What is the minimum baseline?
    - Corrupt PEPs hide their identity using associates and complex corporate vehicles to disguise their beneficial ownership of funds so may not always show up on any watch list - then what?
    - Take reasonable measures to establish the source of wealth and source of funds – is simply asking the question sufficient? Should further due diligence be conducted to confirm the source of wealth / funds?

We look forward to further discussion on this subject.