

# Private-Sector Anti-Money Laundering Databases

An analysis of privacy issues for Canadian financial institutions

March 31<sup>st</sup>, 2011

# Private-Sector Anti-Money Laundering Databases

*An analysis of privacy issues regarding the use of private-sector anti-money laundering databases employed by Canadian financial institutions*

© Copyright 2011 – Her Majesty the Queen in Right of Canada  
All rights reserved.

## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>1. Background.....</b>	<b>4</b>
1.1 Foundation.....	4
1.2 Canada's Sanctioned Individuals & Entities.....	8
1.3 National Databases .....	12
1.4 Non-Governmental Organisations Databases .....	14
1.5 Private Sector Databases .....	15
<b>2. Sanctions List Scrubbing .....</b>	<b>16</b>
2.1 Service .....	16
2.2 Types of Scrubbing.....	16
2.3 Methods.....	17
2.4 Privacy considerations.....	18
<b>3. PEP / PEPF lists.....</b>	<b>19</b>
3.1 Sources of information .....	19
3.2 Distribution .....	21
3.3 Privacy considerations.....	21
<b>4. Persons of Special Interest .....</b>	<b>22</b>
4.1 Sources of information .....	22
4.2 Privacy considerations.....	23
<b>5. ManchesterCF .....</b>	<b>24</b>

## Executive Summary

---

1. ManchesterCF was retained by the Office of the Privacy Commissioner of Canada to examine the subject of private sector anti-money laundering database providers for possible areas of concern in relation to Canada's Privacy Act.
2. Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act places obligations on financial institutions in Canada to examine money laundering and terrorist financing risks for new and existing customers.
3. Politically Exposed Persons ("PEPs") receive enhanced due diligence by financial institutions around the globe. In Canada, financial institutions need only ascribe enhanced due diligence to Politically Exposed Foreign Persons ("PEFPs"), therefore domestic PEPs avoid scrutiny in Canada but not abroad.
4. Due to the complexity of managing sanctions databases and PEP/PEFP requirements issued by governments around the globe, many financial institutions in Canada will outsource these functions to a private sector anti-money laundering database provider.
5. Sanctions lists can present issues regarding privacy if a Canadian is removed from the sanctions list by a national government but then remains in the database of a private sector anti-money laundering database provider as a "person of special interest".
6. There do not appear to be any appeals processes nor privacy policies regarding individuals on these databases, nor any indication that an individual has any legal recourse except to sue for removal from such a database.
7. Some of these firms maintain databases for "persons of special interest" to financial institutions. The determination of who is classified as a "person of special interest" is not generally known and would be considered proprietary by the firm and unfit for public circulation.
8. If an individual's name is submitted by a financial institution to a private sector anti-money laundering database provider and is flagged as a "person of special interest", that individual may be denied financial services as a result of the flag.
9. OPCC may wish to send a letter of enquiry to private sector anti-money laundering database providers, enquiring if they have any arbitration procedures for delisting a name, or any privacy policies that govern their analysis and disclosure to financial institutions operating in Canada.

# 1. Background

---

## 1.1 Foundation

ManchesterCF Consulting Co. Ltd. ("ManchesterCF")<sup>1</sup> was retained by the Office of the Privacy Commissioner of Canada ("OPCC")<sup>2</sup> to investigate the use of private sector anti-money laundering databases by financial institutions in Canada for possible privacy issues.

Combatting money laundering and terrorist financing is an important priority for any civilised society. Laws and regulations must be enacted in order to prevent the abuse of a nation's financial system by organised crime and terrorist groups.

In 2000, Canada enacted legislation to guide financial institutions in combatting money laundering and terrorist financing, namely the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA")<sup>3</sup>.

Canada's financial intelligence unit – the Financial Transactions Reporting and Analysis Centre of Canada ("FINTRAC")<sup>4</sup> – forms an integral component of the government's defences against financial crime, both domestic and international.

Canada has been a member of the Financial Action Task Force ("FATF")<sup>5</sup> since 1990, an organisation founded on providing policy guidance to governments around the globe.

### **Financial Action Task Force (FATF)**

#### **Overview**



*The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The Task Force is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.*

*Since its creation the FATF has spearheaded the effort to adopt and implement measures designed to counter the use of the financial system by criminals. It established a series of Recommendations in 1990, revised in 1996 and in 2003 to ensure that they remain up to date and relevant to the evolving threat of money laundering, that set out the basic framework for anti-money laundering efforts and are intended to be of universal application.*

---

<sup>1</sup> <http://www.manchestercf.com>

<sup>2</sup> <http://www.priv.gc.ca>

<sup>3</sup> <http://laws.justice.gc.ca/PDF/Statute/P/P-24.501.pdf>

<sup>4</sup> <http://www.fintrac-canafe.gc.ca>

<sup>5</sup> <http://www.fatf-gafi.org>

The FATF publishes a list of forty recommendations on anti-money laundering and nine special recommendations on counter-terrorist financing<sup>6</sup>. For the purposes of this analysis, two recommendations are of particular interest, namely Recommendations 5 and 6, as they address two critical issues in fighting money laundering and terrorist financing: customer due diligence and politically-exposed persons.

### **FATF Recommendation 5**

#### **Customer due diligence and record-keeping**



*Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:*

- *establishing business relations;*
- *carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;*
- *there is a suspicion of money laundering or terrorist financing; or*
- *the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.*

*The customer due diligence (CDD) measures to be taken are as follows:*

- a. *Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information*
- b. *Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.*
- c. *Obtaining information on the purpose and intended nature of the business relationship.*
- d. *Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.*

*Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence.*

---

<sup>6</sup> <http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF>

In other words, a fundamental component in any anti-money laundering or counter-terrorist financing regime is that financial institutions thoroughly understanding with whom they are doing business, whether an individual or a corporation, as potential money launderers and financiers of terrorism can be avoided as customers to the financial institution.

Across the globe, cases abound where individuals holding political office – or their families – have become involved in major money laundering or terrorist financing cases. In 2010, the FATF released a reference guide entitled *FATF Corruption Information Note*<sup>7</sup>, outlining how the 40+9 FATF recommendations can be employed to reduce the level of corruption in a nation's economy. The note pays particular attention to "politically-exposed persons", or PEPs.

### **FATF Corruption Information Note**

*Financial service providers must put in place appropriate risk management systems to determine whether a (potential) customer or the individual who ultimately owns or controls the customer is a politically exposed person (PEP). When doing business with a PEP, financial service providers must take reasonable measures to determine the PEP's source of wealth and funds. Such measures increase the possibility of detecting instances where public officials and other persons who are (or have been) entrusted with prominent public functions in a foreign country — such as Heads of State, senior politicians, senior government judicial or military officials, senior executives of state-owned corporations and important political party officials—are abusing their positions for private gain (Recommendation 6).*



The FATF's Recommendation 6 is dedicated to enacting special procedures within a financial institution regarding PEPs.

### **FATF Recommendation 6**

#### **Politically Exposed Persons**



*Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:*

- a. *Have appropriate risk management systems to determine whether the customer is a politically exposed person.*
- b. *Obtain senior management approval for establishing business relationships with such customers.*
- c. *Take reasonable measures to establish the source of wealth and source of funds.*
- d. *Conduct enhanced ongoing monitoring of the business relationship.*

<sup>7</sup> <http://www.fatf-gafi.org/dataoecd/59/44/46252454.pdf>

In Canada, the PCMLTFA makes reference to politically-exposed foreign persons, or PEFs, not PEPs, therefore individuals who would be considered domestic politically-exposed persons are not covered by the PCMLTFA. FINTRAC defines PEFs in its guidelines based on the PCMLTFA regulations.

## **FINTRAC Guideline 6G: Record Keeping and Client Identification for Financial Entities<sup>8</sup>**

**July 2010**

### **7. Politically Exposed Foreign Person Determination and Related Records**

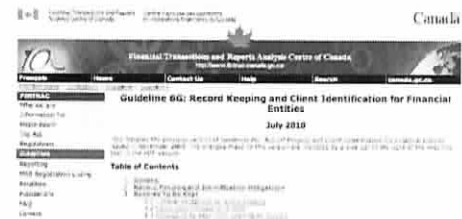
*A politically exposed foreign person is an individual who holds or has ever held one of the following offices or positions in or on behalf of a foreign country:*

- a head of state or government;
- a member of the executive council of government or member of a legislature;
- a deputy minister (or equivalent);
- an ambassador or an ambassador's attaché or counsellor;
- a military general (or higher rank);
- a president of a state-owned company or bank;
- a head of a government agency;
- a judge; or
- a leader or president of a political party in a legislature.

*A politically exposed foreign person also includes the following family members of the individual described above:*

- mother or father;
- child;
- spouse or common-law partner;
- spouse's or common-law partner's mother or father and
- brother, sister, half-brother or half-sister (that is, any other child of the individual's mother or father).

*An individual or family member described above is a politically exposed foreign person regardless of their citizenship, residence status or birth place.*



<sup>8</sup> <http://www.fintrac-canada.gc.ca/publications/guide/Guide6/6G-eng.asp> - s7



Canada's banking regulator, the Office of the Superintendent of Financial Institutions ("OSFI") expands on the distinction of PEPs, rather than domestic PEPs.

### **Office of the Superintendent of Financial Institutions**

#### **B-8 Guideline: Deterring Money Laundering and Terrorist Financing (December 2008)<sup>9</sup>**

*The FATF Recommendations state that PEPs are potentially more susceptible to financial crime than other clients of financial institutions. In Canada, the PCMLTFA requires FRFIs<sup>10</sup> to determine, in prescribed circumstances, whether they are dealing with PEPs and also prescribes mandatory enhanced due diligence measures to be taken in respect of PEPs in prescribed circumstances.*

*A PEP is defined in the PCMLTFA as an individual who holds or has ever held prescribed offices or positions in or on behalf of a foreign state or is a prescribed member of the family of such a person. For purposes of the foregoing, the term "foreign state" should be interpreted to include the principal political subdivisions of foreign countries when applying the PEP definition.*

*Once the determination is made, prescribed actions must be taken within minimum time periods.*

A financial institution operating in Canada would be compliant with the PCMLTFA regulations relating to PEPs if it had a definitive list of the names of all PEPs around the globe, yet no definitive list is issued by any Canadian government entity, nor any entity approved by the Canadian government. Financial institutions are left to their own devices in determining who qualifies as a PEP. It is up to all reporting entities into FINTRAC to understand what constitutes a PEP and whether or not a new or existing customer should be classified as a PEP.

Financial institutions operating in Canada must therefore determine who qualifies as a PEP or engage a third-party firm to assist the financial institution in determining whether a new or existing customer should be classified as a PEP.

## **1.2 Canada's Sanctioned Individuals & Entities**

Databases on individuals sanctioned by the state are maintained by several countries. The United States, Australia, New Zealand, the United Kingdom and the European Union are often cited as countries at the forefront of imposing sanctions upon individuals and organisations deemed a threat due to their linkages with either money laundering, terrorist financing or both.

In Canada, Public Safety Canada publishes a list of sanctioned entities that present risks to the national security of Canada. Financial institutions are barred from providing products and services to these entities.

---

<sup>9</sup> [http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b8\\_e.pdf](http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b8_e.pdf)

<sup>10</sup> FRFIs – Federally Regulated Financial Institutions



## Public Safety Canada

### About the listing process<sup>11</sup>

The Anti-Terrorism Act provides measures for the Government of Canada to create a list of entities that:

- have knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity
- knowingly acted on behalf of, at the direction of or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity

[...]

The process of listing begins with criminal and/or security intelligence reports on an entity disclosing the reasonable grounds to believe that the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or the entity is knowingly acting on behalf of, at the direction of or in association with, an entity involved in a terrorist activity.

Banking regulators around the globe publish lists of entities and individuals who face economic sanctions in the domestic financial services industry. OSFI publishes two lists of interest to financial institutions operating in Canada; one list on sanctioned entities and one on sanctioned individuals. This list can be readily downloaded from the OSFI website in spreadsheet format or in text format for adoption into automatic customer due diligence computer systems.

<sup>11</sup> <http://www.publicsafety.gc.ca/prg/ns/le/atlp-eng.aspx>

## Office of the Superintendent of Financial Institutions

### Terrorism Financing<sup>12</sup>

*Lists of Names subject to the Regulations Establishing a List of Entities made under subsection 83.05(1) of the Criminal Code, and/or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST) and/or United Nations Al-Qaida and Taliban Regulations (UNAQTR)*

indstip\_e.xls

	A	B	C
1	Consolidated List of Names subject to the Regulations Establishing a List of Entities made under subsection 83.05(1) of the Criminal Code or the Regulation		
2	or the United Nations Al-Qaida and Taliban Regulations		
3	PART A - INDIVIDUALS (print version)		
4	Names added to the list in March 2011 are in bold. Updated information on aliases and dates of birth are likewise bolded.		
5			
6	Last Name	First Name(s)	Title/designation/dob/pob/aka/nationality/passport no./national id
	Waziri	Mohammad Jawad	Designation: UN Department, Ministry of Foreign Affairs of the Taliban regime; POB: Cent
413	Yandarbiyev	Zelimkhan Ahmedovich	DOB: 12/09/52; POB: Vydriha Village, Shemonaikhskiy (former Verkhubinskiy) District, E Kazakhstan, USSR; aka: Abdul-Muslimovich, Hussin Mohamed Di Tamimi; Nationality: R; Russian Foreign passport number 535884942; Russian Foreign passport number 35388841
414	Yasin	Abdul Rahman	Grozny City, Chechen Republic, Russian Federation; Other Information: Confirmed to have DOB: 10/04/80; POB: Bloomington, Indiana, United States of America; aka: Abdul Rahms Yasin, Aboud Yasin, Nationality: United States of America; Passport no.: 27082171 (U.S.A. (Iraq). National identification: SSN 156-92-9858 (United States of America); Abdul Rahms
415	Yassin	Ahmed Ismail	Title: Sheik; DOB: 1938; POB: al-Jawrah, al-Majdal District, Gaza

On March 23<sup>rd</sup>, the *Freezing Assets of Corrupt Foreign Officials Act* ("FACFO") was given Royal Assent and entered into force in Canada.

### Freezing Assets of Corrupt Foreign Officials Act<sup>13</sup>

*FACFO permits, at the request of a foreign State, the Government of Canada to take measures in respect of the property of designated officials and former officials of the foreign State and persons associated with them. These officials and former officials and persons associated with them are referred to as politically exposed foreign persons (PEFPs).*

Currently enacted against PEPs from Tunisia and Egypt, the Act bars financial institutions operating in Canada from dealing with individuals listed at the Department of Foreign Affairs and International Trade ("DFAIT") website<sup>14</sup>.

In other words, financial institutions must monitor lists of sanctioned entities and individuals from Public Safety Canada, OSFI and DFAIT. Failure to monitor these lists can lead to administrative monetary penalties from a regulatory body or enforced management or operational changes.

A recent administrative monetary penalty from FINTRAC illustrates the costs of a transgression of the PCMLTFA regulations by a reporting entity regarding customer due diligence and/or PEPs.

<sup>12</sup> [http://www.osfi-bsif.gc.ca/osfi/index\\_e.aspx?ArticleID=524](http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?ArticleID=524)

<sup>13</sup> [http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/issues/sanctions/FACRAnotice\\_e.pdf](http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/issues/sanctions/FACRAnotice_e.pdf)

<sup>14</sup> [http://www.international.gc.ca/sanctions/tunisia\\_egypt-tunisie\\_egypte.aspx?lang=eng](http://www.international.gc.ca/sanctions/tunisia_egypt-tunisie_egypte.aspx?lang=eng)

**February 18, 2011**

***FINTRAC issues an administrative monetary penalty against a savings and credit union<sup>15</sup>***

Ottawa, February 18, 2011 – The Financial Transactions and Reports Analysis Centre of Canada has assessed an administrative monetary penalty against a savings and credit union. The penalty was imposed for violating the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Peoples Credit Union Limited, a savings and credit union in Innisfil, Ontario, was issued a penalty of \$37,090 on February 2, 2011, for committing nine violations:

[...]

- Failure of a prescribed person or entity, in respect of the activities considered by that the person or entity to pose high risk, to take prescribed special measures, which is contrary to subsection 9.6(3) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and section 71.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.

[...]

- Failure of a financial entity to take reasonable measures within the prescribed period to determine whether a person for whom the financial entity opens an account is a politically exposed foreign person, which is contrary to subsection 9.3(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and paragraph 54.2(a) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.

In a case in the United Kingdom, punitive actions were levied by the banking regulator – the Financial Services Authority – against both the firm and a person, the firm's money laundering reporting officer ("MLRO") Michael Wheelhouse.

***FSA fines firm and MLRO for money laundering controls failings<sup>16</sup>***

**29 October 2008**

The Financial Services Authority (FSA) has today fined Sindicatum Holdings Limited (SHL) £49,000 and its money laundering reporting officer (MLRO), Michael Wheelhouse, £17,500 for not having adequate anti-money laundering systems and controls in place for verifying and recording clients' identities. This is the first time the FSA has fined a money laundering reporting officer.

The FSA found a number of failings including:

---

<sup>15</sup> <http://www.fintrac-canafe.gc.ca/publications/nr/pn-ap-eng.asp?n=13>

<sup>16</sup> <http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/125.shtml>

- the firm failed to implement adequate procedures for verifying the identity of its clients;
- it failed to verify adequately the identity of a significant number of its clients;
- it failed to keep adequate records with regard to the verification of the identity of its clients; and
- Mr Wheelhouse failed to take reasonable steps to implement adequate procedures for controlling money laundering risk.

William Amos, head of retail enforcement at the FSA, said:

*"It is vital to the integrity of the UK's financial markets that regulated firms are not used by criminals to launder money. Senior management must implement and follow procedures that meet our requirements so that the risks their firms face are properly managed."*

*"This fine is a warning to firms and individuals about the importance of complying with our rules in this area and we will not hesitate to clamp down on failures, where necessary."*

*In deciding the penalty for SHL, the FSA took into account the limited financial resources of the firm and its ability to pay the fine. Had it not been for these factors the penalty would have been significantly larger.*

Other financial institutions, such as Banco Delta Asia<sup>17</sup> in Macau, China, have faced a similar fate.

In order to protect their businesses from the cost of violating sanctions against individuals or entities, financial institutions will check a new or existing customer's name against a database of high-risk individuals as determined by either a government agency, an international non-government organisation or a private sector firm in the business of providing financial crime risk management services to financial institutions.

## 1.3 National Databases

Governments in various countries maintain databases of known money launderers and financiers of terrorism. Financial institutions operating in the jurisdictions of these governments must ensure they follow the various laws and regulations that apply to these databases, as economic sanctions can be imposed on firms that do not follow the rules.

The two most important national databases are from the United States, the United Kingdom and the European Union, as the economies of both entities are so critical to the international financial system that no financial institution would wish to be excluded from these markets as a result of failings in their anti-money laundering or terrorist financing compliance regimes.

In the United States, the Office of Foreign Assets Control ("OFAC") issues lists of sanctioned individuals by the United States government.

---

<sup>17</sup> <http://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx>

### **United States Treasury – Office of Foreign Assets Control<sup>18</sup>**

*The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.*

*OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction.*

*Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.*



For the United Kingdom, Her Majesty's Treasury maintains its sanctions list within the Asset Freezing Unit.

### **HM Treasury - Financial sanctions<sup>19</sup>**

*The Asset Freezing Unit in the Treasury is responsible for the implementation and administration of international financial sanctions in effect in the UK, for domestic designations under the Terrorist Asset-Freezing etc. Act 2010 and licensing exemptions to financial sanctions.*



Critics argue that domestic financial institutions monitoring of such lists issued by foreign governments constitutes a financial invasion of a nation's sovereign economy. This extra-territoriality is a by-product from the global financial system's dependence on certain reference currencies, namely the United States dollar ("USD"), the European Union euro ("EUR") and the British pound ("GBP").

Both domestic Canadian financial institutions and foreign financial institutions operating in Canada will pay strict attention to the extra-territoriality of these three sanctions regimes, as none of these financial institutions could afford the direct and indirect costs facing those financial institutions who are found in breach of these sanctions regimes.

<sup>18</sup> <http://www.treasury.gov/ofac>

<sup>19</sup> [http://www.hm-treasury.gov.uk/fin\\_sanctions\\_index.htm](http://www.hm-treasury.gov.uk/fin_sanctions_index.htm)

**United States Treasury – Office of Foreign Assets Control<sup>20</sup>**

***Treasury Identifies Lebanese Canadian Bank Sal as a “Primary Money Laundering Concern”***

2/10/2011

*Treasury Acts to Protect the U.S. Financial System from Bank with Ties to a Global Narcotics Trafficking and Money Laundering Network and Hizballah*



WASHINGTON – The U.S. Department of the Treasury today announced the identification of The Lebanese Canadian Bank SAL together with its subsidiaries (LCB) as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act (Section 311) for the bank's role in facilitating the money laundering activities of an international narcotics trafficking and money laundering network. This network moves illegal drugs from South America to Europe and the Middle East via West Africa and launders hundreds of millions of dollars monthly through accounts held at LCB, as well as through trade-based money laundering involving consumer goods throughout the world, including through used car dealerships in the United States. Treasury has reason to believe that LCB managers are complicit in the network's money laundering activities. Today's action also exposes the terrorist organization Hizballah's links to LCB and the international narcotics trafficking and money laundering network.

On March 3<sup>rd</sup>, 2011, it was announced by the Lebanese Central Bank Governor Riad Salameh that Lebanese Canadian Bank would be acquired by a banking unit of Societe Generale, a major international French bank<sup>21</sup>.

## **1.4 Non-Governmental Organisations Databases**

The most widespread non-governmental organisation databases in use by both financial institutions and governments around the globe are determined and maintained by the United Nations<sup>22</sup>. These databases contain sanctions on a variety of individuals and groups, including but not limited to the following:

- UN Security Council Resolution 1267 (1999) concerning Al-Qaida and the Taliban and Associated Individuals and Entities
- UN Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea
- UN Security Council Committee established pursuant to resolution 1737 (2006) on the Islamic Republic of Iran

---

<sup>20</sup> <http://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx>

<sup>21</sup> <http://www.reuters.com/article/2011/03/03/lebanon-bank-idUSLDE7222G420110303>

<sup>22</sup> <http://www.un.org/sc/committees/>



The web of designated individuals and entities on the above lists encompass large amounts of data on the names, alias, birthdates and other information on sanctioned individuals.

## 1.5 Private Sector Databases

By examining the amount of due diligence required by a financial institution on their client base, it becomes rapidly apparent that a market emerges to advise financial institutions in Canada and around the globe on performing customer due diligence and investigating whether a potential or existing client is a politically exposed person, either foreign or domestic.

Services offered by private-sector firms to financial institutions in Canada and around the globe include the following:

- i. Sanction list scrubbing
- ii. PEP / PEPF list intelligence gathering and maintenance
- iii. Determination of persons of special interest

Numerous companies around the globe serve financial institutions seeking to outsource some of their duties under various national anti-money laundering and counter-terrorism financing compliance regimes.

Below is a list of some of the larger firms providing private-sector database services to financial institutions in Canada and abroad<sup>23</sup>.

Provider	Website
World-Check	<a href="http://www.world-check.com">http://www.world-check.com</a>
Dow Jones	<a href="http://www.dowjones.com">http://www.dowjones.com</a>
Oracle Mantas	<a href="http://www.oracle.com">http://www.oracle.com</a>
Detican NetReveal	<a href="http://www.deticanetreveal.com">http://www.deticanetreveal.com</a>
Mongoose Global Intelligence	<a href="http://www.mongoosegi.com">http://www.mongoosegi.com</a>
Complinet Thomson Reuters	<a href="http://www.complinet.com">http://www.complinet.com</a>
Verafin	<a href="http://www.verafin.com">http://www.verafin.com</a>
LexisNexis	<a href="http://www.lexisnexis.com">http://www.lexisnexis.com</a>

At a minimum, all of the above firms provide services that consist of some form of due diligence of a person or organisation against all or more of the aforementioned databases.

---

<sup>23</sup> Firms are not listed in any particular order.



## 2. Sanctions List Scrubbing

---

### 2.1 Service

The sanctions list scrubbing service on offer by the various private sector anti-money laundering database firms is to provide a single source solution to performing basic due diligence on the financial institution's customers.

Enquiries on a particular customer name are generally scrubbed against a master database that is an amalgamation of all the individual country and non-government organisation databases made available by banking regulators and financial intelligence units around the globe.

The private sector anti-money laundering database firm assumes the responsibility for keeping this database current on new designations and the delisting of names removed from sanctions lists. Various pricing models exist to accommodate the numerous types of sanctions list scrubbing stages within a financial institution's operations.

### 2.2 Types of Scrubbing

For financial institutions, managing customers and their requirements involves two types of due diligence:

#### *1. Relationship management due diligence*

- Due diligence when the customer first begins their relationship with the financial institution, usually at the account opening step
- On-going due diligence during the lifetime of the customer's relationship with the financial institution at a frequency determined by the financial institution's risk management function's assessment of anti-money laundering and counter-terrorist financing risks for that customer
- Name scrubbing of individuals managing or owning firms who are investment banking customers in mergers, acquisitions or private equity

#### *2. Transactional due diligence*

- Name scrubbing for non-customers as applicant or beneficiary on inbound or outbound payments, including North American real time gross settlement systems and SWIFT MT103<sup>24</sup> electronic funds transfers in and out of Canada
- Name scrubbing during transmission of trade finance<sup>25</sup>, mocatta<sup>26</sup> or other types of non-payment SWIFT messages

---

<sup>24</sup> Society for Worldwide Interbank Financial Telecommunication ("SWIFT") – <http://www.swift.com>

<sup>25</sup> Such as letter of credit advising, where the beneficiary may not be a customer of a bank

<sup>26</sup> Precious and base metals trading is known within international banking as "mocatta"

## 2.3 Methods

Generally speaking, there are three methods for scrubbing customer names against the private sector anti-money laundering databases:

### 1. *Single inquiry*

- An employee at a financial institution calls up a secure<sup>27</sup> webpage provided by the private sector anti-money laundering database provider
- A customer name is entered by the employee
- A response is generated the browser on whether the name or aliases appear on the sanctions databases of various countries and non-government organisations

### 2. *Straight-through processing inquiry*

- The employee opens an account for the customer
- The computer system data fields containing this new customer information are formatted into data files for transmission
- The data files are sent to the private sector anti-money laundering database provider for basic due diligence scrubbing

### 3. *Batch inquiries*

- Select fields with the customer database are batched together and aggregated into one enormous database
- The database transmitted to the private sector anti-money laundering database provider
- The database is scrubbed against the private sector anti-money laundering database provider

The business models of various private sector anti-money laundering database providers will vary slightly against the scenarios above, however the basics will remain the same.

---

<sup>27</sup> 128-bit Secure Socket Layer encryption embedded in an internet browser is the standard for secure internet banking in Canada. Symantec, one of the leading internet security firms describes it as follows:

#### **What is Secure Sockets Layer or SSL?**

The Secure Sockets Layer (SSL) is a security protocol used by Web browsers and Web servers to help users protect their data during transfer. An SSL Certificate contains a public and private key pair as well as verified identification information. When a browser (or client) points to a secured domain, the server shares the public key with the client to establish an encryption method and a unique session key. The client confirms that it recognizes and trusts the issuer of the SSL Certificate. This process is known as the "SSL handshake" and it can begin a secure session that protects message privacy and message integrity.

- <http://www.verisign.com/ssl/ssl-information-center/ssl-basics/index.html>

In all of the above methods, if a customer's name produces a red flag, an alert is sent to the Chief Anti-Money Laundering Officer ("CAMLO") for further information and possible investigation.

Determinations can then be made on the accuracy of identification and whether or not a suspicious transaction report should be transmitted to the financial intelligence unit.

In Canada, if a financial institution identifies a potential new customer as being listed on a country's sanctions list and denies the person a business relationship with the financial institution, a suspicious transaction report based on an attempted transaction must be filed with the financial intelligence unit.

## 2.4 Privacy considerations

The service offered by private sector anti-money laundering databases of sanctions list scrubbing employs information widely available to the general public, let alone financial institutions. All the websites referenced above where sanctions lists can be downloaded are available to the general public.

The concentration of that information in one firm does not present any privacy issues. It can be argued that since the private sector anti-money laundering database provider has an economic interest in maintaining a professional and current database, there is an economic incentive to ensure that the information is entirely accurate.

The only real privacy consideration that can be raised on sanctions list scrubbing is the possibility that an individual who was placed on a nation's sanctions list and then removed could still be placed on a private sector anti-money laundering database under the provision of "Persons of Special Interest" (see below).

The individual would have a great deal of difficulty determining whether or not their name had been delisted from a private sector anti-money laundering database, as most firms would likely reply to any enquiry from a formerly-sanctioned individual with a stock reply: *"We do not comment on the contents nor the determinations made to produce our databases."*

In an overview of the websites of various private sector anti-money laundering database providers, there was no indication that an appeal or application for removal process was made available to the public.

In such circumstances, the only option remains a civil lawsuit for an injunction to remove an individual's name from the database.

### 3. PEP / PEFP lists

#### 3.1 Sources of information

Banking regulators, government policy makers and financial intelligence units will rarely – if at all – provide a financial institution with an actual list of politically-exposed persons, the names of their spouses, family members and business associates.

The only exception in Canada appears to be the Freezing Assets of Corrupt Foreign Officials Act mentioned in Section 1.2.

#### SCHEDULE 1

##### (Section 2)

#### POLITICALLY EXPOSED FOREIGN PERSONS (TUNISIA)

1. Zine El Abidine ben Hadj Hamda ben Hadj Hassen BEN ALI (also known among other names as Zine El Abidine Ben Ha; Hamda Ben Ha; Hassen BEN ALI), born on September 3, 1936, in Hammam Sousse, son of Selma HASSEN and spouse of Leila TRABELSI
2. Leila Bent Mohamed ben Rhouma TRABELSI (also known among other names as Leila Bent Mohamed Ben Rhouma TRABELSI), born on October 24, 1956, in Tunis, daughter of Saïda DHRIF and spouse of Zine El Abidine BEN ALI
3. Moncef Ben Mohamed ben Rhouma TRABELSI (also known among other names as Moncef Ben Mohamed Ben Rhouma TRABELSI), born on March 4, 1944, in Tunis, son of Saïda DHRIF and spouse of Yamina SOUAI
4. Mohamed ben Moncef ben Mohamed TRABELSI (also known among other names as Mohamed Ben Moncef Ben Mohamed TRABELSI), born on January 27, 1980, in Sebha, Libya, son of Yamina SOUAI and spouse of Ines LEJRI

#### ***Freezing Assets of Corrupt Foreign Officials (Tunisia and Egypt) Regulations<sup>28</sup>***

*Whereas Tunisia and Egypt have asserted to the Government of Canada, in writing, that each of the persons listed in the annexed Freezing Assets of Corrupt Foreign Officials (Tunisia and Egypt) Regulations have misappropriated property of Tunisia or of Egypt, as the case may be, or have acquired property inappropriately by virtue of their office or a personal or business relationship and have asked the Government of Canada to freeze the property of those persons;*

*Whereas the Governor in Council is satisfied that each of those persons are politically exposed foreign persons in relation to Tunisia or Egypt, as the case may be;*

*Whereas the Governor in Council is satisfied that there is internal turmoil or an uncertain political situation in Tunisia and Egypt;*

*And whereas the Governor in Council is satisfied that the making of the annexed Freezing Assets of Corrupt Foreign Officials (Tunisia and Egypt) Regulations is in the interest of international relations;*

*Therefore, His Excellency the Governor General in Council, on the recommendation of the Minister of Foreign Affairs, pursuant to subsections 4 (1) to (3) of the Freezing Assets of Corrupt Foreign Officials Act, hereby makes the annexed Freezing Assets of Corrupt Foreign Officials (Tunisia and Egypt) Regulations.*

<sup>28</sup> [http://www.international.gc.ca/sanctions/tunisia\\_egypt\\_regulations-reglements\\_tunisie\\_egypte.aspx?lang=eng](http://www.international.gc.ca/sanctions/tunisia_egypt_regulations-reglements_tunisie_egypte.aspx?lang=eng)

Within these regulations, a total of 48 individuals from Tunisia and 21 individuals from Egypt are named. Aside from these 69 names, no arm of the Canadian government issues a list of PEPs for use by Canadian financial institutions. Financial institutions and private-sector anti-money laundering database providers are left to their own devices in determining who qualifies as a PEP.

Private-sector anti-money laundering database providers will go to great lengths in order to produce quality databases of PEPs or PEPs for financial institutions in Canada and around the globe.

#### **About the World-Check PEP database<sup>29</sup>**

*More than 75% of the world's leading Financial Intelligence Units (FIUs) have access to World-Check's PEP risk intelligence. World-Check emphasises quality, rather than quantity, and sets out to aid organisations in identifying and mitigating actual PEP risk, rather than merely "ticking the boxes" and confirming the position of a PEP. Thousands of new profiles are added to the World-Check PEP database each month, whilst older ones are constantly updated as new public source data becomes available.*

*Widely recognised as the industry pioneer and thought leader in the field of PEP due diligence and risk mitigation, World-Check CEO David Leppan is frequently called upon to address top-level industry conferences as a keynote speaker on PEP-related issues and challenges.*

#### **Detica NetReveal<sup>30</sup>**

*Detica NetReveal® is a major provider of solutions for sanctions and Politically Exposed Persons (PEP) screening, with over one billion financial relationships being screened globally each day. The Detica NetReveal® (formerly Norkom) solution enables financial institutions to comply with major national and international regulations, avoid regulatory sanction and protect business reputation and viability. Detica NetReveal® sanction and PEP screening enables their clients to meet regulatory requirements in over one hundred countries every day.*

##### *A global regulatory solution*

*The sanctions, PEP and foreign and corrupt practice lists that a typical global institution must monitor have increased in number and size to in recent years, typically 30-40% growth year-on-year. The Detica NetReveal® sanctions and PEP screening supports over 300 regulatory global watchlists and comes pre-packaged with support for leading consolidated list vendors namely World-Check, Dow Jones Watchlist and Accuity, greatly simplifying the challenge faced by organisations in remaining compliant and giving them flexibility to adapt to the future. Furthermore, Detica NetReveal® supports both internal monitoring and fraud watchlists.*

##### *Packaged efficiency and effectiveness*

*With a global footprint across North America, Europe, Asia Pacific and the Middle East, Detica NetReveal® has proven packaged accuracy across the globe. We provide the broadest and deepest set*

---

<sup>29</sup> <http://www.world-check.com/politically-exposed-person-pep-compliance/>

<sup>30</sup> <http://www.deticanetreveal.com/solutions/banking/sanctions-pep-a-314a.html>

*of packaged processes and algorithmic innovations in the market.*

*The Detica NetReveal® sanction and PEP screening is packaged to enhance detection efficiency and effectiveness. It can screen over 60 languages and character sets, which leads to fewer false positives. The Detica NetReveal® sanction and PEP screening also leads the field in investigation efficiency with >90% of all determinations being achieved via a single mouse click.*

Generally speaking, the names of PEPs/PEFPs are registered in the master database within the private-sector anti-money laundering database provider, however they are clearly marked as a PEP/PEFP and whether or not the individual is listed on one or more sanctions lists disseminated by one or more countries.

## 3.2 Distribution

As the PEP/PEFP database is usually integrated with the overall sanctions database, the distribution of PEP/PEFP determinations follows the same architecture as the sanctions database outlined in Section 2 above.

Some private sector anti-money laundering database providers will provide a separate database of PEP/PEFP determinations, however the practical applications of a separate PEP/PEFP database are somewhat limited. Financial institutions generally seek an integrated solution to their compliance requirements, so the demand for separate PEP/PEFP databases is somewhat limited.

## 3.3 Privacy considerations

Under the current PCMLTFA, only individuals designated as foreign politically exposed persons are proscribed for enhanced due diligence by financial institutions. Financial institutions in Canada are not currently required to perform enhanced due diligence on Canadians would be classified as domestic politically exposed persons.

If a foreign national were to approach the OPCC regarding privacy issues concerning their classification as a foreign politically exposed persons, jurisdiction issues would come into play.

It would be difficult for a foreign national to lay claim to privacy issues if they had been classified as a PEFP and enhanced due diligence by a financial institution in Canada had caused them concern for their privacy rights in Canada.

In Canada, persons who would be classified as PEPs would receive enhanced due diligence by financial institutions outside of Canada regarding their financial activity. As this financial activity occurs abroad, it is doubtful that the domestic Canadian PEP would have cause to bring about a complaint to the OPCC.

## 4. Persons of Special Interest

---

### 4.1 Sources of information

Aside from official sanctions lists by both governments and non-government organisations and PEPs/PEFPs, private sector anti-money laundering database firms will monitor “open sources” to identify possible high risk persons from the perspective of money laundering and/or terrorist financing risks to a financial institution.

#### ***Dow Jones***

##### ***Persons of Special Interest***<sup>31</sup>

*Avoid dealing with the wrong person with details of high profile people, not on an official list, but reported in publicly available sources as being accused or convicted of serious crimes including corruption, financial crime, organized crime, terror, trafficking and war crimes.*

#### ***World-Check***

##### ***Due Diligence Reports***<sup>32</sup>

*Compliance with ever increasing privacy laws and regulation is at the heart of what we do and, with this in mind, we have a strict policy that only publicly available records are accessed and used in the course of our research. However, this does not mean that we only use digitised information. Most public records held outside of the developed economies are not in an electronic format and will be filed on paper in the local language.*

*[...]*

*Teams of multilingual researchers based around the world methodically monitor hundreds of thousands of information sources globally creating and updating thousands of profiles on a round-the-clock. Our Data-File is updated twice daily ensuring our customers always have the latest intelligence available.*

The two quotes above do not represent a comprehensive perspective from the entire industry, however they are from two of the largest private sector anti-money laundering database firms employed by financial institutions in Canada.

In summary, analysts at firms in the private sector are combing through vast quantities of data – both electronic and otherwise – to build profiles of what they interpret as “high-risk” individuals. The

---

<sup>31</sup> [http://www.factiva.com/collateral/files/dj\\_watchlist\\_brochure\\_2008.pdf](http://www.factiva.com/collateral/files/dj_watchlist_brochure_2008.pdf)

<sup>32</sup> <http://www.world-check.com/enhanced-due-diligence/>



opinions of these analysts are then passed on to financial institutions once an data field enquiry from a financial institution matches the “person of special interest” data.

A red flag based on this information could severely impact an individual’s ability to access financial services in Canada, as account opening could be denied and an individual’s banking, insurance or asset management relationships could be terminated based on this information.

## 4.2 Privacy considerations

This narrow segment of the private sector anti-money laundering database provider’s product offering is the one area that contains potential privacy concerns.

Information is being compiled on an unknown number of Canadians by analysts at foreign and domestic firms based on assumptions regarding their risk level for potential money laundering and terrorist financing activity.

There does not appear to be any limitations on what information is being collected and how it is being incorporated into an analysis of an individual’s risk assessment for possible money laundering and / or terrorist financing risk, nor any provision for possible error management nor appeals by individuals who may be wronged in the process.

In extreme cases, individuals could be flagged as “persons of special interest” due to their economic activities, such as trading with a nation that is receiving negative press, or from their political affiliations and assumed connections to terrorist groups. Such determinations would be made behind closed doors within the private sector anti-money laundering database provider and would impose very real economic consequences upon an individual who had not been convicted in a court of law for any predicate offense to money laundering or terrorist financing.

Whether the open source information is correct or not, it is a strong factor in an anonymous analyst’s decision on whether or not to include the Canadian individual in the overall database of the private sector anti-money laundering database provider.

The very fact that an individual’s name is included in such a database suggests that they are not low-risk, but at least medium- if not high-risk. Were a financial institution in Canada to have one of their potential or existing customers flagged as a “person of special interest”, it would undoubtedly cause intense scrutiny of the individual’s business relationship with the financial institution, leading to a potential exit in the relationship or limitation on the transaction types that a financial institution would offer the individual.

Individuals with similar names could be flagged as false positives in such databases, potentially causing them harm in their business relationships with financial institutions in Canada and around the globe. This scenario is a common occurrence with air travel and terrorist “no-fly” databases<sup>33</sup>.

The OPCC may wish to consider sending a letter of enquiry to each of the private sector anti-money laundering databases that offer their services to financial institution in Canada on whether or not they have privacy policies in place for their databases related to “persons of special interest”.

---

<sup>33</sup> See 60 Minutes segment “Unlikely Terrorists On No Fly List” –  
<http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml>



## 5. ManchesterCF

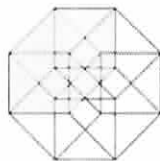
ManchesterCF provides financial crime risk management training programs, advisory services and project management to financial institutions and government agencies around the globe.

For samples of computer-based training, training DVDs and course overviews, please visit the Client Login section of the ManchesterCF website:

<http://www.manchestercof.com>

Founded in 2004, senior principals at ManchesterCF have managed projects in North America, Asia, Australia and Europe for financial institutions, financial intelligence units, government policy makers and supervisory agencies. Projects include:

- Research on money laundering typologies
- Development of risk management products
- Financial crime risk management in emerging markets
- Advisory services to financial institutions on regulatory risk management
- Advisory services on the risk-based approach to financial intelligence units
- Operations re-engineering for financial crime risk defences



### MANCHESTERCF CONSULTING CO. LTD.

Suite 501, 125 - 720 King Street West  
 Toronto, Ontario, Canada M5V 3S5  
 +1 (416) 388 6051  
<http://www.manchestercof.com>

