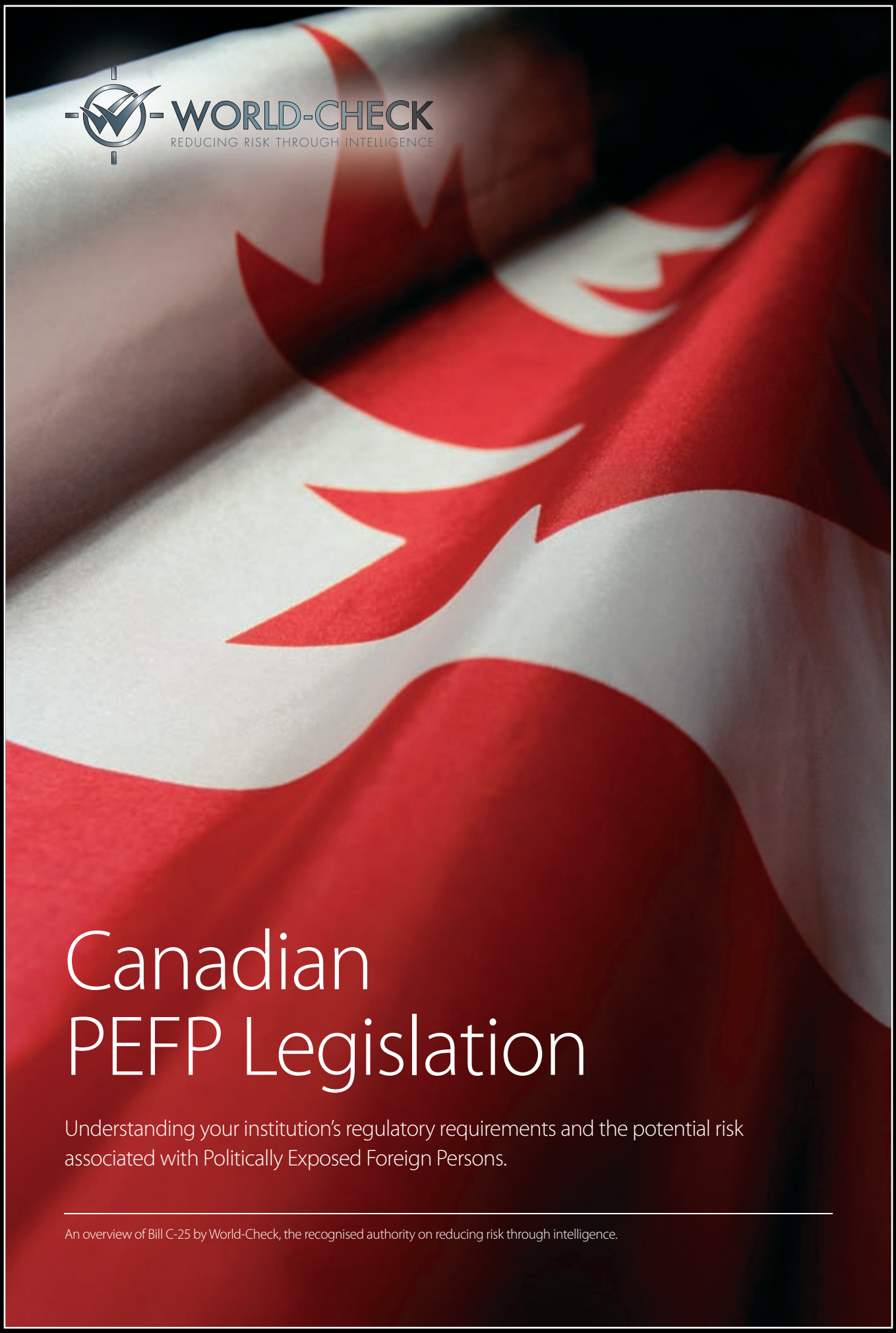


Canadian PEFP Legislation

Understanding your institution's regulatory requirements and the potential risk associated with Politically Exposed Foreign Persons.

An overview of Bill C-25 by World-Check, the recognised authority on reducing risk through intelligence.

Contents

1. Introduction

Constantly evolving terrorism financing, money laundering and organized crime risks have led to the international revision of regulatory standards, and the unprecedented adoption of cross-border compliance legislation in Canada and around the world. Is your institution ready to meet the regulatory challenge?

Is your institution a Reporting Entity?

Canadian regulators require the following institutions and business entities to abide by Bill C-25's compliance stipulations:

- Financial institutions
- Trust and loan companies
- Accountants
- Law firms
- Crown corporations selling money orders or accepting deposits
- Securities dealers
- Credit unions
- Cooperative credit societies
- Foreign exchange dealers
- Life insurance companies and brokerages
- Casinos

Legislative landmarks such as the USA PATRIOT Act and the EU Third Money Laundering Directive set global standards for Know Your Customer, Anti Money Laundering and Counter Terrorist Financing procedures, and form the legislative foundation for country-specific regulations around the world.

Canadian legislators have followed suit with Bill C-25, aligning Canada's legislative framework and enforcement regime with internationally upheld AML and CFT standards. Appropriate risk management practices for dealing with Politically Exposed Foreign Persons (PEFPs) form a key focus area of the bill, signalling the need for Canadian Reporting Entities to prioritize reputational risk management as a matter of urgency.

Falling under Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act, Bill C-25 applies to the full range of reporting sectors, including financial entities, the real estate sector, securities dealerships, forex dealerships, money services providers, accounting firms and even precious gem and stone dealerships.

The Canadian government's successful enforcement of the bill is intended to result in more effective detection and prevention of terrorism financing, money laundering and related financial crime, whilst simultaneously closing existing loopholes.

This far-reaching bill, enacted as a response to the Financial Action Task Force's 2007 assessment of Canada's compliance performance, holds significant implications for Canadian institutions – especially in terms of non-compliance. As of June 23, 2008, failure to comply with Bill C-25's PEFP due diligence requirements carries potential penalties of up to $500,000. But beyond the financial penalties that can be incurred, non-compliant Reporting Entities face a far greater risk – that of reputation damage.

Becoming known as the 'bank of choice' for heightened-risk PEFPs will undoubtedly have a negative impact on an institution's share value and marketplace standing – well beyond the regulatory fines. In essence, PEFP risk is the very real possibility of losing clients, millions of dollars in brand equity, or – even worse – having your correspondent banking relationships terminated and your institution's financial services license revoked.

As a result, Canadian Reporting Entities will have to start taking PEFP screening seriously – and fast.

2. Bill C-25 at a glance

In terms of key changes to Canada's AML/CFT legislation, the following points warrant mention:

- Introduction of expanded due diligence and suspicious transaction reporting requirements for new sectors such as precious stone and metal traders, lawyers and even real estate developers
- Enhanced client identification measures, most notably where foreign customers are not physically present during transactions
- Adoption of a risk-based approach to client due diligence
- Enhanced due diligence and reporting requirements, most notably for dealing with shell banks and Politically Exposed Foreign Persons (PEFPs)
- Creation of an administrative and monetary penalties regime to better enforce compliance with the Act
- Requirement of new and expanded record-keeping as proof of due diligence
- New record-keeping requirements for information accompanying cross-border electronic fund transfers (EFTs)
- Development and implementation of a Money Services Businesses Registry

3. Understanding the implications

Beyond increased reporting and administrative requirements, the biggest challenge represented by Bill C-25 is the requirement for Canadian institutions to screen their relationships with PEFPs.

New legislation clearly demands Enhanced Due Diligence when it comes to PEFPs, but how are compliance professionals meant to identify PEFPs and more critically, those individuals exposed or associated to them?

What exactly is a PEFP, and what are the underlying risks in dealing with these individuals and entities?

The issue lies in the very concept and definition of 'PEFPs'. An in-depth understanding of the PEFP concept is required to successfully implement efficient KYC and Due Diligence programs that will identify not only the PEFP status of an individual, but the 'potential' risk attached to them.

Identifying a PEFP is only the initial step. Enhanced Due Diligence requires that further checks and investigation needs to take place in order to gain insight into an individual or entity's relationship network, objectives and source of funds. Only with the necessary intelligence at hand will institutions be able to make informed decisions about doing business with prospective clients who are PEFPs.

In essence, knowing that a PEFP is a PEFP is not enough; what institutions need is a risk resource that highlights the potential hidden risks carried by PEFPs and their associates. World-Check covers both national and foreign Politically Exposed Persons (i.e. PEPs and PEFPs) with intelligence aimed at highlighting any potential risk surrounding the individual or entity, rather than just confirming a person or entity's PEP or PEFP status.

At the heart of all risk mitigation considerations lies the desire by all institutions to protect their hard-earned reputations. Laws and regulations aside, it makes good business sense to know who you are dealing with.

This document aims at dissecting the PEFP definition in order to provide Canadian institutions with a clearer understanding of the issue, whilst providing answers and solutions. As the pioneer and industry benchmark for KYC intelligence, World-Check has a proven record and many years of experience in providing institutions around the world with the necessary intelligence and tools to carry out effective KYC and Due Diligence procedures. As the industry standard in PEFP screening, World-Check serves more than 3 000 institutions in 162 countries. Significantly, World-Check's client base also includes hundreds of government agencies and 47 of the 50 largest banks in the world.

Dissecting the 'PEP and 'PEFP' definitions

According to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), a "PEFP is a person who holds, or in the past held, one of the following offices or positions in or on behalf of a foreign country (i.e. not Canada)":

- Heads of government or state
- Members of the executive council of government
- Members of a legislature
- Deputy ministers or equivalent positions
- Ambassadors, attachés or counsellors to an ambassador
- Military officers with a rank of general or higher
- Presidents of state-owned companies
- Presidents of state-owned banks
- Heads of government agencies
- Judges
- Leaders or presidents of political parties represented in a legislature

The Canadian PEFP definition also includes the following family members:

- Spouse or common-law partner
- Children
- Parents
- Mother-in-law and father-in-law of spouses or common-law partners
- Children of the PEFP's mother or father (brother, sister, step-brother, step-sister)

In order to gain a deeper understanding of Canadian PEFP regulation and its operational implications, similar pieces of national legislation warrant scrutiny. In accordance with the USA PATRIOT Act, for example, American regulators abide by the definition of a 'Senior Foreign Political Figure':

> *"Current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials; a senior official of a major foreign political party; and a senior executive of a foreign government-owned commercial enterprise. This definition also includes a corporation, business, or other entity formed by or for the benefit of such an individual. Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources.*
> *Also included in the definition of a senior foreign political figure are immediate family members of such individuals, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure."*
>
> ***Extract from FINCEN fact sheet on Section 312 of the USA Patriot Act***

In fact, both Canada's Politically Exposed Foreign Person (PEFP) and the US PATRIOT Act's definitions show a large degree of overlap with FATF's Politically Exposed Person (PEP) definition:

FATF: "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories."

In essence, what Canadian legislation considers a 'PEFP' is simply a 'PEP' from a foreign jurisdiction.

The difference therefore between a PEP and a PEFP, in an operational sense, relates primarily to the regulator's location. For the Canadian regulator, a Nigerian statesman is a PEFP; from a worldwide regulatory perspective, he is just a PEP. Canadian institutions will therefore need to screen all prospective clients against the full PEFP definition using a global PEP database that covers Politically Exposed Persons (PEPs) native to all foreign jurisdictions.

But what about Canadian PEP nationals?

Outside of Canada, financial institutions around the world are required under their equivalent PEP legislation to screen for all PEPs, domestic or foreign. Canadian regulations, however, do not require that their national PEPs be checked or screened for potential risk.

Consider the following scenario: a Canadian financial institution with international presence will have to carry out Enhanced Due Diligence (EDD) on Canadian PEPs in their international branches, however the same level of scrutiny is not necessary for Canadian PEPs in their national operations.

One could convincingly argue that the prevalence of money laundering, corruption and bribery in Canada is nowhere near as high as in some other countries, and that its level of PEP risk is thus considerably lower. But realistically, is any country 100% free of these issues?

> "…PEPs that come from countries or regions where corruption is endemic, organized and systemic seem to present the greatest potential risk; however, it should be noted that corrupt or dishonest PEPs can be found in almost any country".
>
> ***FATF Typology Report 2003/2004***

Moreover, your institution will face the same public scrutiny and reputational damage for dealing with a corrupt Canadian PEP. In fact, ties to a corrupt Canadian PEP could arguably be more damaging than ties with a foreign PEP. Canadian institutions have consequently started adopting the policy of screening for the full spectrum of PEPs - both foreign and domestic – simply because it pays to know who all your PEPs are.

National PEPs have historically been subject to lower levels of regulatory scrutiny,

in part because heightened-risk *PEFPs* tend to conduct transactions in jurisdictions other than their own. Having said this, it is critical to utilise a PEFP intelligence solution that identifies local and foreign PEP risk, both for conducting general KYC due diligence and complying with specific PEFP regulation.

PEP/PEFP status: visibility vs. seniority

One of the most crucial areas in the definition of the PEP/PEFP concept, and one most open to local interpretation, is the extent to which low-ranking officials and public officeholders should be included.

The FATF definition focuses predominantly on 'senior' officials. The Wolfsberg Group, an association of 12 leading global banks, provides the following alternative definition in their recently published "FAQs on PEPs", published in May 2008:

> *"Financial Institutions should consider a range of factors when determining whether a particular holder of a public function has the requisite seniority, prominence or importance to be categorized as a PEP. Relevant factors could include examining the official responsibilities of the individual's function, the nature of the title (honorary or salaried political function), the level of authority the individual has over governmental activities and over other officials, and whether the function affords the individual access to significant government assets and funds or the ability to direct the awards of government tenders or contracts".*

The lack of a more precise official definition of where the line should be drawn with regards to seniority has left Reporting Entities with the challenging task of having to draw the lines themselves. FATF clearly outlined that its definition does not cover "middle ranking and more junior officials", hence the issue is: where does 'senior' stop and 'middle ranking' start?

Consider the following example:

The broad industry consensus used to be that mayors should not be classified as 'senior' public servants. This would indeed be accurate if one is thinking of the mayor of a small town. But surely the mayors of large and capital cities should be included?

Although cities such as St Petersburg, Lagos or New York are not capitals, these are nonetheless influential and wealthy cities. Surely if the mayor of a large, wealthy city wanted to open an account at your institution you would want to carry enhanced due diligence and monitor the account closely?

Thus the PEFP definition evolves and expands over time, driven by common sense

and industry requirements.

World-Check PEFP intelligence is relied on by more than 18 000 compliance and legal professionals worldwide. In collating risk intelligence, its global research team takes cognizance of the requirements by which regulators will judge their clients' compliance efforts, whilst applying the industry knowledge gained from years of dedicated research in this field.

Understanding the regulatory framework that informs PEFPs compliance is key to providing the right intelligence; the lack of such understanding has led to serious shortcomings in other databases.

For example:

- Some PEFP intelligence vendors cover political figures, yet omit known associates (which is where the real risk often lies)

- Some vendors equate associates with family members (whilst family members are a part of the definition, they are often not the vehicles used for illicit transactions. Who would wish to put their own family members at risk?)

- Some PEFP databases don't included source links, leaving clients exposed to legal risk if their data is inaccurate

- Some intelligence vendors don't focus on tracking companies and trusts, despite the fact that these are often used as fronts for transactions. It is not only individuals you should be looking for; companies and trusts can also be 'politically exposed'

Key to World-Check's success is its in-depth understanding of PEP risk. Our expertly trained researchers know exactly what to look for in identifying potential areas of regulatory and reputational risk. If a business associate of an American PEP were to walk into your bank tomorrow to open an account, it may be virtually impossible to determine that this request carries a PEFP risk, based on the identity documents he or she will submit.

How can you therefore identify this potential risk?

4. Understanding where the potential risk lies

Clearly the overwhelming majority of PEFPs create no risk to your organisation. However, it remains a fact that governments and regulators the world over have adopted PEP/PEFP legislation, because PEFPs often have access to, or influence over, state funds and assets, and that such access has led in some very high profile cases to fraud and corruption.

What needs to be understood, however, is that PEFPs are not automatically to be treated as 'too risky', as this could be turning down lucrative client relationships, but rather that they may carry a *potential* risk that simply requires ongoing scrutiny.

PEFPs are often high net worth, prestigious individuals, and are therefore sought after as private banking clients. The ideal PEFP client's source of wealth, their public position (or exposed associations) and income-generating activities are transparent and able to withstand regulatory scrutiny. *Not* ensuring that this is the case, however, can destroy your institution's good reputation.

The main task for all Canadian institutions is therefore to identify, understand and monitor this 'potential risk'.

Compounding this challenge is the fact that PEFPs intent on conducting questionable transactions will go to great lengths to conceal their true identities. It is here where World-Check's risk-relevant PEFP intelligence is key to effective risk mitigation. While family members are a key part of the PEFP definition, a substantial portion of all illicit PEFP activity is not run through the PEFP or their immediate family members, but rather through associates, front-men, or representatives.

5. How can you identify PEFP risk?

The most common forms of PEP/PEFP concealment entail the use of an associate or middleman through whom access to the banking system is gained.

Experience has shown that the likelihood of a questionable politician with something to hide sending his or her close family to stand in the account opening queue at a bank is very rare. If the goal is to hide one's identity, it wouldn't make sense to send someone called Charles Taylor Jr to the bank in the foolish hope that no one picks up on the name or questions the millions being transferred in haste from Liberia.

The real risk lies with the middlemen and advisors – the men and women who broker the deals are almost always the ones involved in account openings, either in their own names or on behalf of companies or trusts used as vehicles for the movement of funds, thus warranting increased scrutiny for potential PEFP risk.

Offshore companies, trusts, charities or similar financial or fiduciary vehicles are often exploited to conduct illicit transactions, in fact, the prominent figure and his or her family may arguably be the last individuals you need to watch out for.

Choosing the right PEFP intelligence vendor is essential

Having access to a PEFP database that is nothing more than a listing of government employees and family members will not suffice. At this juncture, risk-relevant foreign PEP intelligence means the difference between effective risk mitigation and the danger of serious regulatory consequences and reputation damage. Institutions need specific risk intelligence that reveals relationship networks and identifies corporate vehicles in order to recognize and understand the true risk landscape surrounding an exposed individual.

Only with the right intelligence at hand will you be able to make the right decisions in order to meet your regulatory requirements and protect your institution's reputation.

Consider the following example to illustrate the importance of having access to risk-relevant intelligence:

Mr X approaches your institution as a prospective client. You start your Due Diligence process with an initial check using a PEFP database.

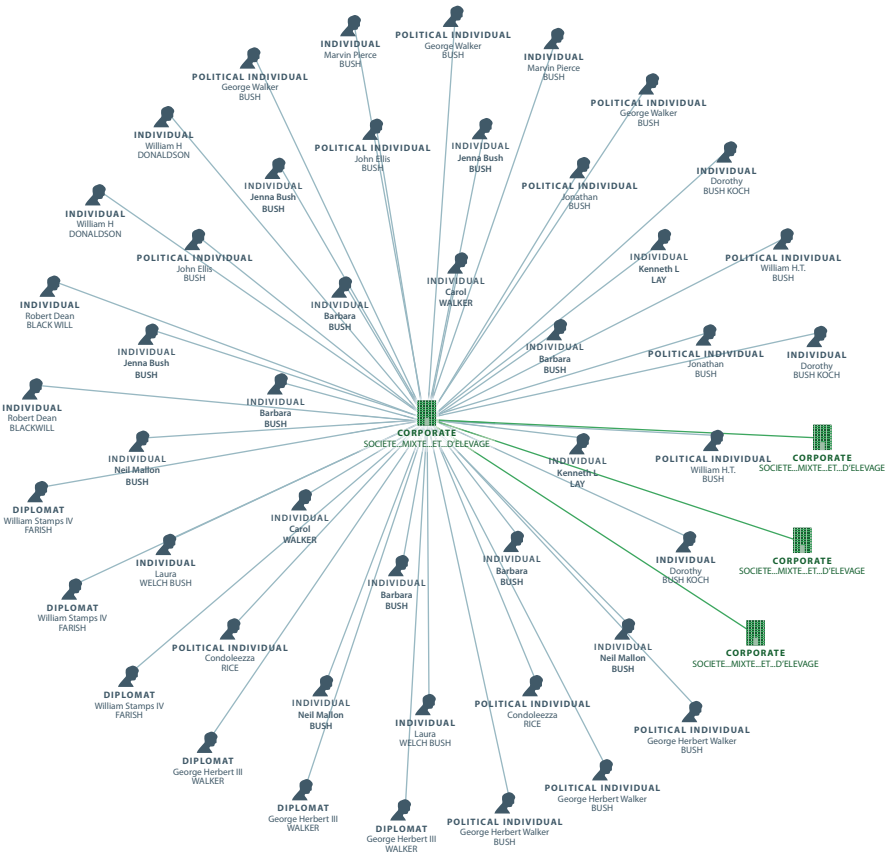
Database Y reveals that Mr X is a PEFP. It confirms that he is the Secretary to the Ministry of Agriculture of a particular foreign country, and it cites the names of his wife and children.

You are thus dealing with a PEFP; but what now? Could you really assess the risks this prospective client carries based on this information? Mr X is most likely just a great high net worth client, but he may also present huge reputational risk.

How can you be expected to make a sound risk management decision without risk-relevant information to help you evaluate the potential risks?

World-Check's intelligence reveals that Mr X is the Secretary to the Ministry of Agriculture of a particular foreign country, that he is married to Mrs X and has two children. But more importantly, it reveals that his associates, Mr T and Mr Z, are currently under investigation for fraud and bribery, and that Mr X has links to 20 different companies and trusts, two of which have alleged ties to a terrorism financing network.

Suddenly, Mr X has taken on a totally new and potentially heightened risk dimension. With the right intelligence at hand, you will be able to weigh the risk and make informed decisions. With limited intelligence, you conversely stand to place your institution's reputation at risk.



6. PEFPs are not just 'people'

A major misconception regarding PEFPs is that one should only be concerned about individuals when identifying PEFP risk.

A FATF consultation paper issued in 2002, indicates that "the proceeds of corruption are typically transferred to a number of foreign jurisdictions and concealed through private companies, trusts or foundations."

There exists a very real possibility that you are already doing business with PEFPs via a legal entity. From a compliance solution perspective, it is key to be able to identify associations between legal entities such as trusts and the persons using these vehicles. Companies can also be Politically Exposed and should therefore be tracked, screened and monitored accordingly.

A database that fails to cover associate entities will not protect your institution from risk, and will not help you meet your regulatory requirements.

Current legislation prohibits any Canadian reporting institutions from entering into a correspondent banking relationship with a shell bank. As such, using a database that covers both individuals and entities is vital.

Identifying 'hidden risk PEFPs', and the importance of regular screening

Given the fact that more than 310 general and by-elections took place worldwide during the period of 2005 to 2007 alone, it is quite likely that a percentage of your existing banking clients may have become politically exposed without your knowledge. In order to mitigate your institution's 'sleeper PEPF' risk, routine re-screening of all existing clients is vital.

When carrying out automated name screening, the below considerations are of utmost importance if the process is to be manageable and cost efficient.

7. PEFP database criteria

Be sure to verify that the PEFP database you're screening against meets the following criteria. Is it:

- **Meticulously structured**

Only a rigorously structured database where not a comma, letter or full stop is out of place, will allow for a seamless integration in an automated environment. Be wary of low price databases. When it comes to implementation, you will see your IT costs sky-rocketing if the database is not 'clean' and properly structured.

Choose a database with a proven track record of delivering results without false-positives.

- **Risk-relevant**

The screening process must deliver the right results and identify actual risk. It is no use screening against irrelevant data that will result in thousands of false positives. You may think you are saving money now on a database that seems to promise it all at low cost, but think of your administrative and remediation costs further down the line, as you'll have to review thousands of false hits. Gathering and maintaining quality PEFP intelligence is a labour-intensive and costly exercise; any vendor offering database access too cheaply should be approached with extreme caution. You will either pay for good data upfront or pay exponentially downstream in the form of substantially higher internal operating costs and the very real consequences of missed hits and hidden relationships.

- **Up to date**

This is vital, so make sure your data provider devotes the necessary resources to keeping its PEFP data up to date on a 24/7 basis.
How many full-time researchers do they have on staff?

- **Global in its coverage**

Canadian regulations require you to check for Politically Exposed Foreign Persons - that is all the PEPs outside of Canada – so be sure to choose a database that is truly global in its coverage.

- **Dynamic**

Depending on your needs, you may wish to screen against certain sub-sets of data: If you intend to carry out an internal investigation on all your Mexican PEFPs, for example, be sure to choose a PEFP vendor that enables you to screen against specific data slices.

- **Verifiable**

Establish whether the sources used to collate risk profiles are cited and accessible

(i.e. URLs and hyperlinks are provided along with the full downloadable database), and whether these sources are of a credible nature. Should the data sources cited prove to be inaccurate, you will be exposing yourself to litigation.

- **Interactive**

Does your PEFP database provider offer a channel through which you can request further investigation on an individual or entity, whether they are included in the database or not?

Does the database cover the following?

- **Entities** (trusts, companies, shell banks, etc.)

This is vital in terms of regulatory and risk management considerations. Make sure the database you use covers entities as well as individuals, as PEFP risk often resides in financial vehicles, rather than with individuals.

- **The full risk spectrum**

Screening your customers for PEFP risk clearly protects your institution from the risks associated with this category, however it is not enough to protect it from the full range of other risks it faces. The most efficient process, currently adopted worldwide by most institutions, is to screen all their customers against all categories of risk in one process.

It is therefore essential that the intelligence database you choose covers all sanction lists, as well as terrorists, fraudsters, narcotics traffickers, human traffickers, arms dealers, and money launderers – in short, the full spectrum of other non-PEFP risk categories. Only then will your institution be able to ascertain exactly what threats are hiding in its customer base. Experience has shown that every institution has its share of skeletons – rather you find out about them before your regulator or the public does.

Meeting regulatory requirements whilst safeguarding your reputation

During the last decade, the substantial increases in regulatory requirements have presented institutions with serious logistical challenges. The responsibilities of remaining compliant are daunting, and the consequences of failure are grim. Having said this, there is a strong business case to be made for adhering to compliance regulations.

Beyond avoiding potential monetary fines or trading sanctions, the process of 'Knowing Your Customer' protects your institution from risks that could lead to reputational damage and the associated loss of brand equity.

No institution wants to have terrorists, money launderers or human traffickers in their client base. Key to addressing these needs is choosing the right intelligence provider.

A good intelligence provider will tell you that Mr A's brother-in-law is an arms dealer, and Mr B's wife is the arms dealer's sister. It will tell you behind which company Mr A's brother-in-law is hiding his activities, and that Mr B is not only a board member and trustee of this company, but also a convicted trafficker of narcotics. This amounts to relevant risk intelligence, which makes for effective due diligence.

Again, a simple database of who is in office (and who their family members are) does nothing but saddle you with issues and escalating IT costs.

8. World-Check: the industry benchmark for KYC intelligence

Since its creation in 2000, World-Check has been at the forefront of PEFP research and KYC intelligence, and as such has taken the lead in providing regulated industries with direction and clarity.

Dedicated researchers, industry experts, regulators, law enforcement leaders and the legal community join World-Check at its annual forums and monthly seminars to collaborate on defining best practice and advancing compliance excellence in the industry.

The truth is that the 'PEFP concept' is a multi-faceted topic. The reason that no official PEFP list exists is that creating, updating and maintaining a global risk-relevant, comprehensive database of PEFPs is an incredibly complex and tedious task – not to mention one that could be influenced by individual government agencies' political sentiments or ruling party allegiances.

Such an ongoing task demands extensive human and technological capital combined with commitment and dedication. It was in meeting this challenge that World-Check has become the industry standard for risk intelligence. No other vendor – or group of vendors, for that matter – come close to matching World-Check's investment in building and managing a PEFP and high-risk entity database. It is this investment that positions World-Check as the industry standard, with over 3 000 clients, including hundreds of government agencies and 47 of the 50 largest banks in the world.

What does it take to become an industry leader?

World-Check's substantial investments in technology and human capital bears testimony to its commitment to providing regulated institutions with the intelligence and tools they need to achieve compliance. But no company becomes the best in the business overnight. It takes:

- Several operational centers across multiple continents, functioning on an uninterrupted 24/7 basis to cover all countries and times zones for emerging risks. World-Check's covers more than 240 countries and territories worldwide

- More than 150 specialised, full-time researchers collating intelligence in more than 35 languages. Each month 20 000 to 22 000 new profiles added, whilst 32 000 to 34 000 profiles are updated on a monthly basis

- Expertly trained PEFP risk researchers gathering risk-relevant intelligence

- A dedicated OFAC and Sanction List Unit to monitor all official lists and ensure that World-Check is updated daily. (World-Check has identified high-risk individuals and entities ahead of OFAC on more than 225 occasions.) World-Check's government coverage includes all Canadian authorities as well

- A highly specialized Terrorism and Insurgency Research Unit (TIRU) tracking and profiling terrorists, insurgents and their financial networks. (World-Check's

database contains more than 28 000 terrorism-related profiles, compared to a total of only approximately 139 terrorism-related entries included in the following prominent Canadian lists: CCC, OFSI, TPS, RCMP, CFSEU and the UNSTR

- A dedicated Data Quality Control team to ensure the 'cleanliness' and meticulous structuring of the data. This data integrity safeguard is vital to ensure glitch-free automation of risk screening processes

- A team of more than 25 dedicated IT professionals that ensures the service is enhanced on a regular basis to meet the emerging demands and requirements of the industry: Dynamic Downloads, Multiple reporting capabilities, Relationship Network Display functionalities, News-Check, Passport-Check, Country-Check, anonymous name reporting – in short, the ceaseless pursuit of excellence and innovation

Intelligence is about connecting dots, but the dots move, change and often cease to exist. Keeping track of this is what makes the difference between a database and an intelligence service. World-Check has the required commitment and passion for uncovering the hidden factors that hold the key to reducing risk: a passion for accuracy, relevance and fairness, and for constantly evolving, improving and developing.

Recommended reading

Refining the PEP definition
Edition II http://www.world-check.com/whitepapers/2008/

Reputation Damage: The Price Riggs Paid
http://www.world-check.com/whitepapers/2006/

From a Different Angle
Collection of articles by Kenneth Rijock - Financial Crime Consultant for World-Check
http://www.world-check.com/articles/2008/06/

"Expert Talk"
Terrorism experts discuss terrorism financing methods
http://www.world-check.com/experttalk/2008/

"Industry Voices"
A collection of articles and critical papers discussing common issues and challenges faced by the compliance community
http://www.world-check.com/industryvoices/2008/

www.world-check.com

About World-Check

Over 3 000 institutions rely on World-Check for their KYC and AML compliance requirements. World-Check's global database of heightened-risk individuals and entities is updated daily in real-time by its international research team, and is derived from hundreds of thousands of public sources. Coverage includes money launderers, financial criminals, terrorists and sanctioned entities, as well as individuals and businesses from more than a dozen other high-risk categories. The database also covers Politically Exposed Persons (PEPs) worldwide. World-Check intelligence and tools find direct application in financial compliance, Anti Money Laundering (AML), Know Your Customer (KYC), PEP screening, Enhanced Due Diligence (EDD), fraud prevention, government intelligence and other identity authentication, background screening and risk prevention practices. World-Check offers a downloadable database for the automated screening of an entire customer base, as well as a simple online service for quick customer screening. If you are looking for results, look no further – with a 97% annual client renewal rate, the facts speak for themselves.