Beyond the Checklist

Anti-Money Laundering, Sanctions and Corruption Concerns for the Insurance Sector
Introduction

In this white paper, we explore key risks, mitigating measures and critical considerations for the design, implementation and improvement of an AML/CFT compliance program for insurance companies.

Notwithstanding decades of legislative and regulatory focus on anti-money laundering (AML) and combating the financing of terrorism (CFT) across the globe, financial institutions continue to struggle to meet compliance expectations. Why?

As money laundering (ML) and terrorist financing (TF) methods become ever more sophisticated in an increasingly interconnected global financial system, regulators’ expectations continue to evolve. To satisfy their regulatory obligations, financial institutions must go beyond templates and checklists to develop a deeper understanding of the dynamic risks of their markets, products, customer bases and intermediaries.

Although high-profile money laundering cases have centered on banking organizations’ failures, money laundering cases in the insurance industry are increasing.¹ The multitrillion-dollar insurance sector is particularly vulnerable to money laundering due to its size, the easy availability and nature of its products, and the structure of its business. Products can be purchased across borders and are distributed via brokers or other intermediaries, while the beneficiaries of covered policies are different from the policyholders, making customer due diligence difficult.

This paper does not seek to provide a comprehensive view of AML rules for insurance companies around the world, but rather focuses on the environment in select countries in three regions: North America, Europe and Asia–Pacific.

AML/CFT Regulatory Framework: Overview of Key Measures and Considerations

The Financial Action Task Force (FATF) established a comprehensive legislative and regulatory framework — the FATF Recommendations — to combat ML and TF, as well as the financing of the proliferation of weapons of mass destruction (WMD). Additionally, in October 2011, and amended in November 2015, the International Association of Insurance Supervisors (IAIS) established 26 global standards for supervising the insurance sector, known as the Insurance Core Principles (ICPs). These standards cover a range of topics, including AML/CFT, anti-corruption, fraud, governance and intermediaries. Consistent with the FATF Recommendations and IAIS ICPs, many countries have implemented AML/CFT laws and regulations for insurance companies (and related intermediaries, such as insurance agents and brokers) offering life and investment-related insurance products. Some countries have expanded AML/CFT requirements to include non-life insurance service providers as well. The following comparisons of U.S. AML/CFT requirements to those of other jurisdictions selected here are intended simply to highlight how requirements may vary and are not intended to be comprehensive.

### NORTH AMERICA

#### United States

The USA PATRIOT Act expanded the Bank Secrecy Act’s (BSA) definition of financial institutions required to establish AML/CFT compliance programs to include companies offering the following high-risk “covered products”:

- Permanent life insurance policies, other than group life insurance policies;
- Annuity contracts, other than group annuity contracts; or
- Any other insurance products with cash value or investment features.

#### Canada

In Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) is applicable to any life insurance companies or foreign life insurance companies that are subject to the Insurance Companies Act (or life insurance companies regulated by a provincial act). Guideline B-8, issued by the Office of the Superintendent of Financial Institutions (OSFI), also applies to federally regulated insurance companies.

Certain recent amendments to the PCMLTFA, published in February 2014 and July 2015 (the draft amendments were finalized in July 2016), were aimed specifically at insurance companies:

- Foreign Branches and Subsidiaries
  - Insurance companies must ensure that any foreign branches and subsidiaries have policies in place similar to those in Canada.
- Politically Exposed Person (PEP)
  - Insurance companies are now required to screen for foreign and domestic PEPs, as well as the heads of international organizations, family members or close associates of such persons.
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) Reporting:
  - The exemption regarding reporting cash transactions of CA$10,000 or more by life insurance companies (for product purchases where the source of funds is not easily identifiable) is being repealed; and
  - Reporting entities will be required to keep a record of any “reasonable measures” they have taken in cases where they were unable to ascertain the information specified.
In the European Union (EU), the Third Anti-Money Laundering Directive (AMLD) identified life insurance and annuities, as well as the following products, as vulnerable to abuse:

- Supplementary insurance carried on by life assurance undertakings — in particular, insurance against personal injury, including incapacity for employment;
- Permanent health insurance (Ireland and the United Kingdom [UK]);
- Operations subject to supervision by the administrative authority responsible for the supervision of private insurance — for example, certain tontines, capital redemption operations based on actuarial calculation and management of group pension funds; or
- Certain operations relating to the length of human life.

Although affected countries will have two years to implement modifications into national legislation, the Fourth AMLD (and further amendments proposed in December 2016, dubbed the Fifth AMLD) impacts the Third AMLD requirements for many types of financial institutions, including insurance companies, providing clarity in the following key areas:

- Risk-based approach (applicable or justified for simplified due diligence [SDD])
- Beneficial ownership (e.g., enhanced record-keeping requirements for owners with more than 25 percent or more control internally and on public/central registers).
- The Fifth AMLD clarifies that EU Member States must be compliant with register requirements within 18 months of the Fifth AMLD implementation date (this has not yet been set, but the EU Parliament is expected to adopt the amendments in June 2017).

While there are no insurance-specific updates, the changes bring the EU’s AML/CFT system further in alignment with the FATF Recommendations.

While the application of specific AML/CFT laws and regulations for insurance companies vary and continue to evolve from country to country, these measures are often similar to those that have been long-established for banks. The following is an overview of some key measures, along with related considerations and examples from multiple jurisdictions:

- Governance and Risk Management Framework
- Customer Acceptance and Maintenance Program
- Suspicious Activity Monitoring Program
- Know Your Employee and Know Your Third Party Programs
- Sanctions Compliance Program

---

United Kingdom

Even though the UK is subject to the Fourth AMLD, in April 2016, the United Kingdom’s Home Office and Her Majesty’s (HM) Treasury issued an Action Plan for anti-money laundering (AML) and counter-terrorist finance (CTF).

The Action Plan, which represents a potentially significant change to the UK’s AML/CTF regime, calls for both the government and the private sector to work together better to build a regime to effectively and efficiently combat ML/TF threats. Integral to the Action Plan’s success is the sharing of information among law enforcement agencies, supervisors and the private sector. The aim is to allow UK businesses to better focus their resources to detect, assess and address serious financial crimes.

Reforming the current suspicious activity reports (SARs) regime and building on the success of the government’s Joint Money Laundering Intelligence Taskforce (JMLIT) pilot will be central to the foundation of a new and more collaborative public-private partnership. This initiative, to be led jointly by the Home Office and the National Crime Agency (NCA), is due to be completed by October 2018.

---

ASIA-PACIFIC

Singapore

In Singapore, the Monetary Authority of Singapore (MAS) Notice 314 — Prevention of Money Laundering and Countering the Financing of Terrorism — Direct Life Insurers outlines AML/CFT requirements for financial services firms. The requirements of the notice apply to a direct life insurer, only in relation to its insurance business concerned with life policies, but excludes the business of providing the reinsurance of liabilities under life policies.

---


Governance and Risk Management Framework

An effective AML/CFT compliance program is robust and dynamic and begins with a strong governance framework. The essential elements for establishing and maintaining an effective governance framework are:

• Strong and evident support from the board of directors and executive management for a culture of compliance, which is reinforced through a clearly defined risk appetite statement, appropriate limits, and the institution’s performance review and compensation decision-making processes, among other ways

• A designated AML/CFT compliance officer with the necessary skills, authority and support to manage the AML/CFT compliance program across the entire organization

• An adequate number of dedicated skilled resources, which will be determined by factors such as the size, complexity and geographic reach of the institution, as well as the extent to which the compliance effort is enabled by technology

• Clear delineation of roles and responsibilities of the first, second and third lines of defense, including obligations for “credible (or effective) challenge”

• AML/CFT training, which is appropriately customized to different audiences within the institution

• Strong working relationships between the AML/CFT compliance organization and other groups within the organization (such as legal and fraud) with which the AML/CFT compliance organization would be expected to interact

• Robust management reporting that includes the necessary metrics to measure and monitor risks and performance

• Ongoing monitoring and periodic independent testing of the effectiveness of the program

• Ensuring robust oversight of third-party reliance arrangements and risk management in certain scenarios.

The development of a risk-based compliance program begins with evaluating the risks of customer types, products and geographies in which the institution and its customers conduct business and developing appropriate measures to mitigate those identified risks. Insurance companies can utilize multiple types of risk assessments (e.g., enterprisewide, line of business/legal entity, geographic, product/service, customer, sanctions) in the design and execution of their compliance programs. Insurance companies may also leverage national risk assessments conducted on a country level by the government(s) of their head office and country of operations to mitigate against existing and emerging ML/TF threats.
Consistent with FATF Recommendation 18, under Section 352, the USA PATRIOT Act requires covered insurers to establish AML/CFT compliance programs that include the following “four pillars,” at minimum:

- Development of written internal policies, procedures and controls
- Designation of an AML/CFT compliance officer
- Ongoing AML/CFT employee training program
- Independent testing of the AML/CFT compliance program

Even though the law does not specifically require insurers to conduct risk assessments, it does require insurers to establish risk-based AML/CFT compliance programs. In 2014, the Financial Crimes Enforcement Network (FinCEN) issued additional guidance on fostering a culture of compliance, highlighting general principles that illustrate how financial institutions and their leadership may improve and strengthen organizational compliance with BSA obligations.  

Insurers may be required to comply with additional AML/CFT laws if they are registered as broker-dealers with the U.S. Securities and Exchange Commission (SEC).

Canada

The PCMLTFA requires financial institutions, including insurance companies, to maintain an AML compliance program with certain minimum components. Furthermore, OSFI, as the primary regulator for federally regulated financial institutions (FRFIs), reiterates the requirement to institute an AML compliance program with the following minimum components that are stipulated in both the PCMLTFA and OSFI Guideline B-8:

- Board and senior management oversight, including reporting to senior management;
- An appropriate individual responsible for implementation of the program (e.g., a chief anti-money laundering officer [CAMLO]);
- Assessment of inherent ML and TF risks with a written methodology;
- Written anti-money laundering/anti-terrorist financing (AML/ATF) policies and procedures that are kept up to date and approved by a senior officer, including control policies and procedures;
- Written ongoing training programs;
- Self-assessment of controls; and
- Effectiveness testing with written supporting procedures.

---

6 The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), ss. 71(2)
7 PCMLTFR p. 71(3)(a)
8 PCMLTFA ss. 9.6(2)
9 PCMLTFR p. 71(3)(b)
10 PCMLTFR p. 71(3)(d)
11 PCMLTFR p. 71(1)(c)
12 PCMLTFR p. 71(3)(e)
## EUROPE

### Italy

In accordance with the EU’s AMLDs and Italy’s Legislative Decree 231/2007, as amended effective January 1, 2105, the Istituto per la Vigilanza sulle Assicurazioni (IVASS), Italy’s insurance supervisory authority, issued further guidance for insurers and intermediaries (e.g., agents, brokers, Poste Italiane) under Regulation 5 concerning:

- Customer due diligence (CDD)
- Recording of data and information
- EDD and identification of beneficial owners
- Obtaining information regarding the scope and nature of ongoing relationships and continuous monitoring.

The regulation provides guidance on the duties and responsibilities of the board of directors/board management, managing director/AML general manager, the board of statutory auditors, the supervisory body and the internal audit function.

Emphasizing the use of a risk-based approach referred to as “proportionality,” the regulation excludes certain products based on type (e.g., supplementary pension schemes without redemption clauses) and threshold (e.g., annual premiums less than 1,000 euros, single premiums less than 2,500 euros).

As with financial institutions in other EU Member States, Italy’s insurance companies will need to leverage national and supra-national risk assessments, the former required under the Fourth AMLD, to enhance their risk-based approach to ML/TF.

## United Kingdom

In the United Kingdom, general insurers have an obligation to report suspicious activity under the Proceeds of Crime Act 2002 (POCA), comply with sanctions legislation and explain the new powers granted to HM Treasury under the Counter-Terrorism Act 2008. General insurers are not within the regulated sector, as defined under the Money Laundering Regulations 2007, but in certain circumstances they are required to report suspicious activity to the NCA. General insurers are advised to set a policy in relation to meeting their obligations under POCA and the Counter-Terrorism Act.

According to the Joint Money Laundering Steering Group’s (JMLSG) guidance for the UK Financial Sector Part II Section 7A (revised in November 2014), general insurers should consider the following:

- Development of internal policies and procedures
- Communication of those policies and procedures to all staff
- Clear and written procedures in place to help staff identify the kinds of activities or customers that might arouse suspicion
- Clear guidance to be given to all staff on the risk and implications of alerting potential or actual customers (or agents thereof) to the fact that a SAR has been submitted (i.e., the “tipping off” provision of POCA)
- Clear guidance to be given to all staff on the risk and implications of failing to report their suspicions
- Short reporting lines between front-line staff and a nominated officer
- Record keeping: Report why the decision was made to file a suspicious claim, and why a decision is taken not to file a SAR
- Screening procedures to ensure high standards for recruitment
- Ongoing employee training to ensure employees recognize suspicious activities and understand the internal procedure for recording suspicious activities
- A system of testing compliance, which should be both independent and adequately resourced.
Key questions about governance and risk management frameworks that insurers should consider include:

- Is there a process to identify the insurer’s critical AML/CFT risks? Are these risks reported to the board or its designated committee(s) to prioritize the board’s risk oversight focus?

- Is the board approving major policy issues on a before-the-fact basis (e.g., mitigating policy measures implemented as AML risks are proactively identified)?

- Is there a process in place for identifying and communicating emerging AML and other fraud risks to enable management and the board to be proactive in responding to them?

- Are significant, unexpected risk issues escalated to executive management and the board on a timely basis?

- How does risk drive the overall AML/CFT strategy (e.g., discontinue or prohibit the provision of high-risk products [e.g., bearer policies] or transaction types [e.g., monetary instruments]; allocation of human and technical resources, design of the customer acceptance and maintenance program, suspicious activity monitoring program, training program, and agent due diligence program)?

- What tone has senior management established for the institution? How is a culture of compliance encouraged in the organization?

- Is compliance and/or senior management surprised by key themes and topics dominating industry conferences and seminars?

- Is there regular (every 12 to 18 months) and independent testing of the program performed by someone outside of the compliance officer and staff?
Customer Acceptance and Maintenance Program

A customer acceptance and maintenance program (e.g., know your customer [KYC], CDD, SDD, EDD generally refers to the steps taken by a financial institution to establish the identity of a customer; understand the nature of a customer’s activities (ultimately, to be satisfied that the source of the customer’s funds is legitimate); and assess the risks associated with that customer, both at the inception of the relationship and on an ongoing basis. In recent years, there has been more focus on identifying the underlying beneficial owners of certain legal entities. Some regulators have insisted on the tracking of relationships (e.g., familial, corporate, transactional) and, under certain circumstances, monitoring customers at the “household” level.

To be effective in mitigating risks, insurers must go beyond verifying identities and analyze customer data in an intrinsic manner to discover the overarching and, at times, underlying narrative. Insurers are required to maintain records for a designated period that can vary between countries and between states within the United States — the average minimum period is five years. Firms need to ensure that they retain all records within those limits and that they comply with data protection laws.

<table>
<thead>
<tr>
<th>NORTH AMERICA</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
</tr>
</tbody>
</table>

Although insurance companies are not required to implement a Customer Identification Program (CIP) in accordance with Section 326 of the USA PATRIOT Act, they collect and verify the name, date of birth, address, identification number (e.g., Social Security number) and other details of customers as a matter of safety and soundness.

Insurers are also expected to implement internal programs and written policies to identify bank customers and to verify their identities. As part of the KYC program, firms need to ensure that they:

- Know the customer type and products that are being used;
- Understand expected activity versus actual activity; and
- Are able to identify beneficial owners.

As part of the CDD/EDD process, firms should periodically review their customers to better understand behavior and any changes of products/services being used. During the periodic reviews, companies should:

- Track if/when a customer transfers ownership or designates a beneficiary;
- Know the customer type and products that are being used;
- Track/monitor the pace of refund premiums, surrenders, redemptions and withdrawals;
- Track the use of policy loans; and
- Update the length of the relationship.
The PCMLTFA and OSFI Guideline B-8, Deterring and Detecting Money Laundering and Terrorist Financing, require insurance companies to implement the CDD processes. CDD is comprised of client identification, information gathering, ascertaining identity and ongoing monitoring.

Life insurance companies are not required to ascertain the identity, or obtain the identification information, of a person where there are reasonable grounds to believe that the person’s identity has been ascertained in the prescribed manner by another life insurance company or life insurance broker or agent in respect of the same transaction or of a transaction that is part of a series of transactions that includes the original transaction. For these situations, life insurance companies should develop and implement policies and procedures designed to ensure that:

- They perform appropriate initial and ongoing due diligence on other life insurance companies, life insurance brokers or agents; and
- There are reasonable grounds to believe that the client identification and verification procedures used by such other life insurance companies, life insurance brokers or agents comply with the PCMLTFA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), and with the life insurance company’s own policies and procedures.

Regulators such as OSFI understand that, with respect to individual products, life insurance companies do receive information about the identity of the client on application forms submitted by life insurance agents or brokers. This practice enables life insurance companies to periodically determine reasonable grounds for relying on such agents.

Many FRFIs rely on introducers, intermediaries, brokers or other third parties for client information gathering and verification purposes.

With respect to this accountability, FRFIs must have an agreement or arrangement in writing with the agent or mandatary if such person is to be responsible for client identification and verification. The provisions of this arrangement or agreement must conform to the requirements of the PCMLTFR, and the agreement should obligate the agent or mandatary to:

- Apply the life insurance company’s client identification and verification requirements (which must comply with the regulatory requirements);
- Ensure that, where the client is present at the time client identification is ascertained, the agent or mandatary applies client identification procedures that include viewing original identification documents;
- Ensure that, where the client is not present at the time client identification is ascertained, the agent or mandatary applies prescribed non-face-to-face identification requirements; and
- Provide the client identification information to the life insurance company promptly after obtaining it.

Life insurance companies should also:

- Ensure that if the agent or mandatary is responsible for collecting the information required to make a third-party determination or a politically exposed foreign person (PEFP) determination, these responsibilities are also documented;
- Periodically review, in a systematic manner, the quality of client information gathered and documented by the agent or mandatary to ensure that it continues to meet their requirements.

- Ensure they receive client identification information in the required time frames; and
### ASIA-PACIFIC

#### Hong Kong

In Hong Kong, the Office of the Commissioner of Insurance (OCI) regulates the insurance sector in accordance with the following key AML/CFT laws:

- **Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO)**
- **Drug Trafficking Recovery of Proceeds Ordinance**
- **Organized and Serious Crimes Ordinance**
- **United Nations (Anti-Terrorism Measures) Ordinance (UNATMO)**

The AMLO establishes CDD and record-keeping requirements, including who must be verified (e.g., beneficial owners, trusts); what information and documentation must be collected; when due diligence must be conducted (e.g., inception and ongoing); and special requirements for specific types of customers (e.g., PEPs, correspondents) and financial institutions.

Insurers are required to record the name(s) of the beneficiaries (or the beneficial owners of a trust/legal entity) whenever a new beneficiary is identified or designated by the policyholder of an insurance policy. Insurers must verify identity at the time the beneficiary exercises a right vested in the beneficiary under the insurance policy or at the time of (first) payout to the beneficiary, whichever is earlier.

#### Singapore

MAS requirements state that a direct life insurer shall perform CDD when: (1) the direct life insurer establishes business relations with any customer; (2) there is suspicion of ML or TF; and (3) the direct life insurer has doubts about the veracity or adequacy of any information previously obtained.

- In certain instances, simplified (e.g., no evidence of AML concerns) or enhanced (e.g., PEPs) CDD is acceptable.
- A direct life insurer shall verify the identity of the customer using reliable, independent source data, documents or information. In cases where the customer is a legal person or legal arrangement, a direct life insurer shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent, source data documents or information.
- A direct life insurer shall also obtain the full name, including any aliases, of such beneficiary or obtain sufficient information concerning the beneficiary to satisfy itself that it will be able to establish the identity of such beneficiary at the time of payout. This includes determining beneficial owner(s) with different guidelines, depending on whether the customer/beneficiary is a legal arrangement or natural person.
• A direct life insurer must monitor its business relations with customers on an ongoing basis as well, including, but not limited to:

  - Observing the conduct of the customer’s life insurance policy and scrutinizing transactions undertaken in the course of business relations to ensure that the transactions are consistent with the direct life insurer’s knowledge of the customer, its business and risk profile, and, where appropriate, the source of funds.
  
  - Paying special attention to all complex, unusually large or unusual patterns of transactions, undertaken in the course of business relations, that have no apparent or visible economic or lawful purpose.
  
  - Establishing and implementing adequate systems and processes, commensurate with the size and complexity of the direct life insurer, to assist with ongoing monitoring.

• Record keeping must be maintained for five years, at a minimum, following completion of the transaction/business with the customer with regard to:

  - CDD information relating to the business relations and transactions undertaken in the course of business relations, as well as policy files, business correspondence and results of any analysis undertaken.
  
  - Data, documents and information relating to a transaction undertaken in the course of business relations, including any information needed to explain and reconstruct the transaction.

• A direct life insurer shall ensure that the CDD data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, connected parties of the customers and beneficial owners of the customers are relevant and kept up-to-date by undertaking reviews of existing CDD data, documents and information, particularly for higher risk categories of customers.

Key questions about customer acceptance and maintenance programs that insurers should consider include:

• How does risk drive the design and execution of the customer acceptance and maintenance program?

• Does the CDD program collect and verify the identities of underlying beneficial owners?

• Is information other than identification collected to assist in understanding the nature of customers’ activities for investigative purposes?

• Does the definition (and identification) of PEPs align with leading best practices and regulatory guidance (e.g., domestic PEPs, inclusion of close associates and legal entities owned/controlled by PEPs, persons employed by international insurers)?

• Are due diligence measures applied appropriately (e.g., in the United Kingdom, automatic entitlements of simplified or basic due diligence should be removed and only applied in confirmed low-risk scenarios)?

• Are records retained in accordance with local record retention and data protection laws and regulations?

Firms should create a consistent and single view of the customer (i.e., the information collected through customer acceptance should speak to information extracted from transaction monitoring, which should incorporate customer risk rating, etc.).

---

Suspicious Activity Monitoring Program

A suspicious activity monitoring program describes processes designed to detect, identify and escalate potentially suspicious activity internally and disclose it externally to appropriate supervisory and law enforcement authorities (e.g., state or national regulators, financial intelligence units [FIUs]). Monitoring is not limited to reviews of transaction activity. Potentially suspicious activity can be detected in other types of customer activities (e.g., provision of fraudulent or inaccurate documentation during the application process).

Historically, suspicious activity reporting from insurance companies has been low (e.g., less than 2 percent of the 1.73 million SARs filed in the United States during 2014 were filed by insurance companies). However, according to the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), this trend may not reflect the true level of money laundering in the insurance sector due to underreporting by insurance companies and/or the filing process (e.g., reports attributed to the filing institution offering the insurance products [e.g., a bank]).

FinCEN has also received reports of suspicious transactions involving the structured purchase of life insurance and annuities, followed by the receipt of checks from life insurance companies and the wiring of the funds to foreign countries. Insurance brokers have also been subjected to regulatory enforcement actions and fines for sanctions breaches.

The scenario on the right touches on several AML/CFT considerations, all interconnected, which insurers need to consider carefully in order to develop further their understanding of the risks inherent in their products and market activities.

---


### NORTH AMERICA

#### United States

In the U.S., insurance companies are required to file SARs with FinCEN on suspicious transactions involving “covered products” only. Insurers are required to report any suspicious transaction when it is over $5,000 and the company knows or suspects that the transaction: (1) is part of any illegal activity intended to hide or disguise funds derived from illegal activities; (2) is designed to evade the BSA; (3) has no apparent lawful purpose; (4) or involves the use of the insurance company to facilitate criminal activity.

#### Canada

In Canada, under FINTRAC Guideline 2: Suspicious Transactions, life insurance companies, brokers and agents must report suspicious transactions and attempted transactions.

A life insurance company is defined as one regulated by provincial legislation or a life company or foreign life company under the Insurance Companies Act. A life insurance broker or agent refers to an individual or entity registered or licensed provincially to carry on the business of arranging contracts for life insurance. The guideline provides money laundering indicators specific to life insurance and annuities products.

The implementation of automated transaction monitoring is not mandatory. However, as part of life insurance companies’ AML/ATF obligations under OSFI Guideline B-8 and FINTRAC Guideline 4, they are required to conduct ongoing monitoring of business relationships. Part of this monitoring involves a review of the transaction history to ensure any suspicious activity has been reported.

### EUROPE

#### Germany

The German Federal Financial Supervisory Authority (BaFin), in consultation with insurers, is considering requiring the implementation of an automated solution to monitor for suspicious activity, even though German law does not explicitly require it. One argument for automation is to mitigate the increased ML/TF risk introduced by the Single Euro Payments Area (SEPA), a European-wide initiative to standardize the way electronic payments are processed in euros. Since payments are processed by International Bank Account Number (IBAN) and Bank Identifier Code (BIC) and banks are no longer required to verify whether a bank account belongs to the stated accountholder, insurers are unable to verify whether the debited bank account belongs to the policyholder. Specific rules/parameters designed to detect suspicious patterns (e.g., frequent micropayments by multiple third parties) within an automated system can mitigate the risks of SEPA and similar payment platforms.
Key questions about suspicious activity monitoring programs that insurers should consider include:

- Are compliance and business-line personnel aware of common or emerging red flags (e.g., FATF, IAIS ICPs, Federal Financial Institutions Examination Council [FFIEC])? Can compliance translate “red flags” into meaningful detection rules/triggers in the suspicious activity monitoring program?

- How is the effectiveness of the monitoring program evaluated (e.g., analysis of alert-to-case and case-to-SAR ratios, reviewing overlap between populations of high-risk customers and alert generators)?

- Whenever possible, are key monitoring functions centralized, or, at least, are monitoring results (e.g., cross-channel alerts) shared among relevant departments, lines of business, global divisions and others?

- Does the suspicious activity monitoring program review customer activity holistically, utilizing all available information to develop an understanding of customer activities? Or is it limited to “covered products” only, excluding other product offerings from other lines of business or affiliates?

- Does the suspicious activity monitoring program include monitoring on a combination of levels (e.g., transaction, product, customer, geographic)? Does it consider both explicit and underlying relationships (e.g., accounts linked through transaction activity)?

- Although not required to determine, confirm or prove the underlying predicate crime (e.g., ML, TF, identity theft, fraud, corruption), are compliance personnel trained to have a basic understanding of certain crimes to assist in detecting and reporting relevant information to law enforcement and FIUs?

- Can the monitoring program detect microstructuring (schemes that are increasingly more common with the introduction of standardized payment methods that can facilitate a high volume of payments with minimal customer information [e.g., SEPA])?

- If implementing an enterprisewide system on a global level, can the solution accommodate different time zones and currencies and apply custom rules/parameters to each jurisdiction? Has the organization considered the impact of different privacy laws and regulations on its ability to obtain and share information on customers?

- Have personnel been trained on leading best practices and legal standards for conducting and documenting investigations (e.g., FinCEN’s “Five Ws” [Who, What, Where, When, Why?]; Hong Kong’s Joint Financial Intelligence Unit’s [JFIU] “SAFE” [Screen, Ask, Find, Evaluate] approach)?
Integration of agents and brokers into an AML/CFT compliance program must go beyond training and the development of policies and procedures to obtain relevant customer-related information from intermediaries.

While contractual responsibilities may vary based on the arrangement with intermediaries (e.g., captive, co-branded dual-employee, third-party networking agreements), brokers and agents must be incentivized to commit to their dual roles as sales representatives and gatekeepers responsible for detecting and reporting potentially suspicious activity.

Beyond monitoring relationships with agents, insurers must also mitigate risks imposed by their reinsurance business and associated underlying third parties (e.g., know your customer’s customer (KYCC)).

Additionally, some countries delineate when and how an insurer may rely upon third parties to execute elements of its compliance program (e.g., conducting due diligence). As with agents, roles and responsibilities should be delineated contractually and continuously monitored for compliance. It is important to note that the insurer is ultimately responsible for its compliance with AML/CFT requirements, whether or not it relies upon a third party.

<table>
<thead>
<tr>
<th>NORTH AMERICA</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>In the U.S., agents and brokers are not required to maintain independent AML/CFT compliance programs under the BSA and USA PATRIOT Act. However, consistent with FATF and IAIS guidance, insurers are required to integrate these intermediaries into the company’s AML/CFT compliance program. Insurers may outsource other elements of their AML/CFT compliance program (e.g., monitoring, collection and verification of customer information, sanctions screening) to third parties under the following conditions:</td>
<td></td>
</tr>
<tr>
<td>• Ensuring they have obtained a written agreement for the services to be performed by the service provider and that the terms of the agreement meet the insurer’s requirements.</td>
<td>• Conducting adequate due diligence on the third party’s AML/CFT compliance program and/or its understanding of AML/CFT requirements.</td>
</tr>
<tr>
<td>• Monitoring the third party’s performance under the contract on a continuing basis.</td>
<td>• Performing adequate due diligence of the third party’s operations on a periodic basis.</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
</tr>
<tr>
<td>Similar to their counterparts in the United States, agents and brokers in Canada are not required to maintain their own AML/ATF compliance program. However, OSFI Guideline B-8 requires that any agents performing customer identification (or any other AML function) be subject to a written agreement and receive adequate training and oversight from the insurance company. For life insurance companies, accountability for ascertaining the identity of the client and obtaining the information used to identify the client remains with the FRFI when it uses a third party to ascertain the identity of clients. With respect to this accountability, FRFIs must have an agreement or arrangement in writing with the agent or mandatary if such person is to be responsible for client identification and verification. The provisions of this arrangement or agreement must conform to the requirements of the PCMLTFR, and it should obligate the agent or mandatary to:</td>
<td></td>
</tr>
</tbody>
</table>
Canada (Continued)

- Apply the deposit-taking institution (DTI) or life insurance company's client identification and verification requirements (which must comply with the regulatory requirements);

- Ensure that, where the client is present at the time client identification is ascertained, the agent or mandatary applies client identification procedures that include viewing original identification documents;

- Ensure that, where the client is not present at the time client identification is ascertained, the agent or mandatary applies prescribed non-face-to-face identification requirements; and

- Provide the client identification information to the DTI promptly after obtaining it.

DTIs and life insurance companies should also:

- Ensure that if the agent or mandatary is responsible for collecting the information required to make a third-party determination or a PEFP determination, these responsibilities are also documented;

- Ensure they receive client identification information in the required time frames; and

- Periodically review, in a systematic manner, the quality of client information gathered and documented by the agent or mandatary to ensure that it continues to meet their requirements.

Other areas to consider:

- Documentation of relationships and communications with, and client due diligence work of, agents and mandataries, should be complete and current, and client information should be placed in the client's record promptly upon receiving it.

- FRFIs should consider terminating relationships with agents or mandataries that do not comply with agreed upon client identification responsibilities or provide the DTI or life insurance company with the requisite client information on a timely basis.

- Contracts with agents and mandataries should be reviewed and updated as necessary to ensure compliance with the PCMLTFR regarding the use of agents and mandataries.

- The extent of the DTI's or life insurance company's exposure to the agent or mandatary for the results of client due diligence should be addressed expressly in the DTI's or life insurance company's inherent risk assessment.

EUROPE

Italy

Italian Legislative Decree 231/2007. Regulation 5, outlines the types of third parties permitted to conduct due diligence on behalf of an insurer (e.g., other banks in Italy and the EU, Poste Italiane, electronic money institutions, brokerage firms) and the role they can fulfill (e.g., all phases of due diligence, only identification and verification of customers).

Insurers are required to define the following:

- The phases of CDD delegated to third parties.

- The data and information that they want to receive from the third parties.

- The tools and timing for the transmission of information flows.

- The operational procedures for the verification of the correctness and reliability of information and of the escalation actions, in case of a negative outcome.

- Where necessary, acquire further information from third parties, the client or other sources.
In Singapore, an insurance company can rely on a third party if:

- The direct life insurer is satisfied that the third party is in compliance with AML/CFT requirements.
- The life insurer takes appropriate steps to identify, assess and understand the ML and TF risks particular to the countries in which the third party operates.
- The third party is willing to provide any data, documents or information obtained with respect to the life insurer’s customer.
  - No insurance company can rely on a third party to conduct ongoing monitoring of its business relations with customers.
- An insurance company can rely on a third party to perform customer due diligence, simplified CDD or enhanced CDD if it documents the basis for knowing the third party complies with AML/CFT requirements and also obtains the CDD information from the third party immediately.

Key questions about know your employee (KYE) and know your third party (KY3P) programs that insurers should consider include:

- How are conflicts between sales and compliance objectives for agents and brokers minimized?
- Is the due diligence program capable of detecting insider abuse (e.g., collusion between clients and agents, agents that may be exploiting their clients for personal gain)?
- Does the due diligence program extend beyond brokers and agents? Could it detect insider abuse orchestrated by senior management?
- Are relied-upon third parties continually monitored for compliance with internal and regulatory requirements?
Sanctions Compliance Program

A sanctions compliance program is often considered a subset of the AML/CFT compliance program, as it typically targets terrorists and terrorist nations, drug traffickers, proliferators of WMDs, and persons involved in corruption-related activities.

To comply with sanctions laws, generally, insurers must screen customers (e.g., policyholders, beneficiaries) and transactions against sanctions listings and, with positive matches, block, reject and/or report assets/transactions to the relevant government authority.

As international efforts to combat drug trafficking, terrorism and the proliferation of WMDs continue to converge, there may be significant overlap between the sanctions lists maintained by different countries, especially by those countries that have ratified the same international instruments to combat transnational crimes (e.g., UN Consolidated Lists, EU Consolidated Lists, HM Treasury Asset Freezing Unit16 Lists).

The more recent noteworthy sanctions settlements by the Office of Foreign Assets Control (OFAC) have involved foreign financial institutions with U.S. operations, further emphasizing the importance of maintaining a robust sanctions compliance program in all relevant jurisdictions.

### NORTH AMERICA

#### United States

The U.S. OFAC administers and enforces economic and trade sanctions, including, but not limited to:

- Counter Terrorism Sanctions Program
- Counter Narcotics Trafficking Sanctions Program
- Transnational Criminal Organizations Sanctions Program
- Non-Proliferation Sanctions Program
- Rough Diamond Trade Controls Sanctions Program
- Country-Based and Regime-Based Sanctions Program (e.g., Iran, Iraq, Libya, North Korea, Russia, Sudan, Syria)

#### Canada

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. These legislative measures apply to all Canadians, including Canadians residing outside Canada, and more particularly to all FRFIs. Compliance with the laws requires that FRFIs implement the following types of control measures:

- Searching in FRFI records for individuals and entities designated by the laws and subject to financial sanctions (e.g., using the UN lists of sanctioned designated nationals);
- Determining whether the FRFI is in possession or control of property of Designated Persons;
- Preventing prohibited activity with respect to property of Designated Persons (by freezing assets) and monitoring for and preventing prohibited transactions;
- Disclosing information to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) concerning property of Designated Persons in the FRFI’s possession or control; and
- Reporting to OSFI monthly on the aggregate value of property of Designated Persons in the FRFI’s possession or control.

---

16 In October of 2007, the responsibility for the administration of financial sanctions in the United Kingdom transferred from the Bank of England Financial Sanctions Unit to HM Treasury Asset Freezing Unit.
The Service for Foreign Policy Instruments (FPI) administers sanctions prepared by the European External Action Service and the Council of the European Union in support of specific EU Common Foreign and Security Policy (CFSP) objectives and United Nations Security Council Resolutions (UNSCR). Types of restrictive measures include, but are not limited to:

- Arms embargoes
- Trade restrictions, such as import and export bans
- Financial restrictions
- Restrictions on movement, such as visa or travel bans

The HM Treasury Asset Freezing Unit watch list contains the names of persons and entities that have been listed by the United Kingdom, as well as by the UN and EU, including those that pose a significant risk of providing support for acts of terrorism.

The JMLSG issued guidance for the UK financial sector regarding AML/CFT and the sanctions regime. Firms are advised to adopt controls and processes in order to comply with sanctions obligations in an effective and proportionate manner in areas including:

- Senior management responsibility
- Staff training
- Screening of customers and transactions
- Tailored/risk-based approach
- Review of processes
- Screening software (legacy systems and fuzzy matching)
- Outsourcing and reliance
- Reporting matches and breaches

Key questions about sanctions compliance programs that insurers should consider include:

- How is the design and execution of the sanctions compliance program based on risk? Firms need to select appropriate watch lists to best align with the institution’s customer base, geographical reach, risk appetite and so on.

- Does the sanctions compliance program consider the sanctions risk of all jurisdictions in which the institution operates?

- Are all parties (e.g., policyholder, beneficiary, payer, underlying third parties in reinsurance contracts) subject to ongoing sanctions screening?

- Do potential matches trigger further investigation beyond confirmation?

- Is the sanctions compliance program capable of detecting willful violations conducted by employees (e.g., deliberate stripping of names to circumvent monitoring systems and freezing/rejecting mechanisms)?

- Are metrics tracked to observe matching effectiveness?
Conclusion

Compared to other types of financial institutions, insurers are generally at lower risk of exposure to ML and TF. However, a lack of awareness about existing AML/CFT risks and obligations can increase the insurance industry’s vulnerability to such activity.

With increasing fines aimed at institutions and personnel, it is even more imperative for insurers to refine their AML/CFT compliance strategies continuously.
HOW WE HELP COMPANIES SUCCED

Protiviti helps insurance companies address their AML/CFT requirements by understanding where ML/TF risks arise and identifying strategies to control and mitigate them. Our Regulatory Risk consulting practice can help insurance companies strengthen their AML/CFT compliance programs by:

• Evaluating the adequacy of policies, procedures and processes given the company’s insurance sales activities, its role in insurance sales and the risks the insurance sales present.

• Assessing whether the controls are adequate to reasonably protect the company from ML, TF and related risks.

• Reviewing the contracts and agreements for networking arrangements with affiliates, operating subsidiaries or other third-party insurance providers conducting sales activities on behalf of the company.

• Depending on the company’s responsibilities as set forth in the contracts and agreements, reviewing management information system (MIS) reports (e.g., large transaction reports, single premium payments, early policy cancellation records, premium overpayments, and assignments of claims) and internal risk rating factors.

• Determining whether the company effectively identifies and monitors covered insurance product sales.

• Determining whether the system for monitoring covered insurance products for suspicious activities, and for reporting suspicious activities, is adequate given the company’s size, complexity, location and types of customer relationships.

• Assisting in the selection of appropriate technology tools to support ongoing AML/CFT and sanctions monitoring, including current and future requirements, vendor review and assessment scorecarding, project planning and management, implementation support, system tuning, and system validation.

• Reviewing account opening documentation, ongoing due diligence information and account activity to determine whether activity is unusual or suspicious (e.g., by comparing anticipated transactions with actual transactions).

• Reviewing existing sanctions compliance programs and making recommendations for enhancements, and assisting in the development, implementation and documentation of an effective sanctions compliance program.

Protiviti can help insurance companies identify the current strengths and weaknesses of their AML/CFT compliance programs by conducting a gap analysis of current compliance procedures to gauge potential exposure to ML/TF risks and noncompliance. Each AML/CFT compliance program can be tailored to match an insurance company’s unique business context, including the organization’s internal infrastructure and external landscape.
THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge
ARGENTINA*
Buenos Aires
BRAZIL*
Rio de Janeiro
Sao Paulo
CANADA
Kitchener-Waterloo
Toronto
CHILE*
Santiago
MEXICO*
Mexico City
PERU*
Lima
VENEZUELA*
Caracas

EUROPE

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRMS