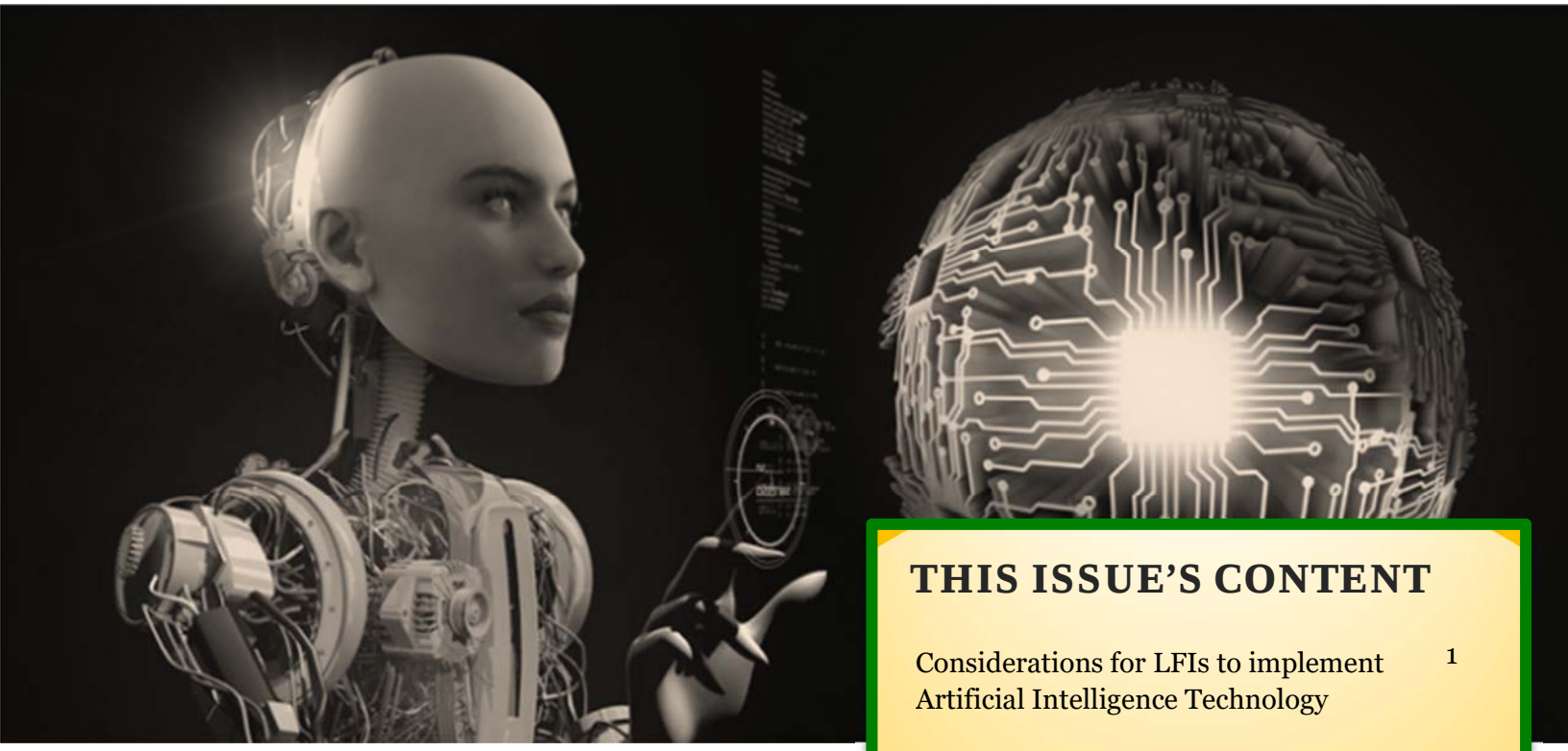
AML/CFT NEWSLETTER

ISSUE 10 JUNE 2023



THIS ISSUE'S CONTENT

NEW AND EMERGING TECHNOLOGIES

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO IMPLEMENT ARTIFICIAL INTELLIGENCE TECHNOLOGY

In the Anti-Money Laundering, Counter the Financing of Terrorism and Proliferation (AML/CFT/CPF) space, artificial intelligence (AI) has grown significantly given its potential to revolutionise AML/CFT/CPF efforts. AI refers to the ability of a computer or computer-controlled systems to think like humans and to perform tasks commonly associated with human beings. With the rapid advancement in digital solutions, and as financial institutions (FIs) seek to remain competitive, AI has no doubt found its way into the banking and financial services sector.

FIs are identifying the benefits and have begun harnessing the power of advanced data analytics, big data, machine learning and natural language processing technology to enhance operational efficiency, improve customer experiences, meet regulatory expectations, and mitigate risks.

AI has the power to improve customer on-boarding and the overall customer service experience. Globally, banks and other FIs have utilised AI solutions to improve their customer service experiences while managing cost, for example with the use of AI-enabled chatbots and voice assistants. AI has also allowed for more streamlined, personalised and automated support in answering queries, and in some cases, even processing transactions quickly and more efficiently.

As FIs embrace digital/non-face channels to interact with customers, the use of AI is becoming increasingly useful in the identification and verification of customer information. Through the use of biometric information, as an alternate to traditional methods of identification and verification, FIs can streamline on-boarding procedures, while ensuring security and accuracy of customer information.

AI solutions can enhance risk-based AML/CFT/CPF programmes and strengthen AML/CFT/CPF risk management. It has the potential to assign more accurate identification of risk categories at on-boarding and throughout the client relationship. AI also has the potential to enhance customer screening and monitoring processes. In addition, AI powered systems have the capability to analyse vast amount of data in real time thus enabling more accurate and efficient assessment of institutional Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF) risk.

When appropriately configured, AI has the potential to strengthen FIs' ongoing monitoring efforts and the identification and reporting of fraudulent activities, anomalies and trends. Digital revolution through the use of AI, machine learning, big data, and natural language technology, has the potential to significantly improve FIs' ability to manage its AML/CFT/CPF risk and meet regulatory obligations.

AML/CFT/CPF compliance consideration for FIs

While FIs are encouraged to explore and take advantage of the benefits of AI, the Eastern Caribbean Central Bank (ECCB) highlights several factors for consideration when deciding on and implementing AI solutions:

1. Establish an AI governance framework;

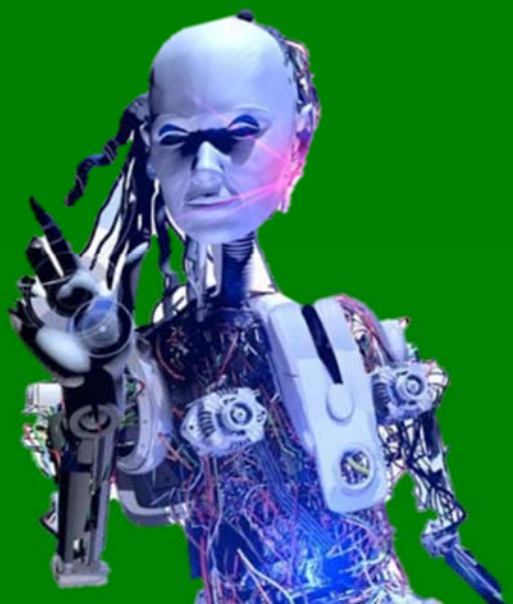
2. Assess the AI system's ability to integrate with the institution's legacy systems;

3. Establish clear policies and procedures around the use of AI;

4. Ensure that use of the AI technology allow for compliance with local and international AML/CFT/CPF laws and regulations, in addition to standards on data protection, privacy, and cybersecurity and other applicable laws and regulations;

5. Monitor AI systems for compliance with applicable laws and regulations; and

6. Inclusion of AI systems within the FI's compliance programme to include:
    - Automated tools to monitor AI compliance;
    - Develop and implement a comprehensive training programme on AI compliance requirements;
    - Integrate into audit plan, auditing for AI systems; and
    - Establish a process for reporting and responding to compliance related issues;



7. Inclusion of risk posed by the use of AI in the risk management programme and strategies; and

8. Ensure complete transparency and traceability within the system.

The ECCB's commitment to support innovation and digital transformation

The ECCB is a strong advocate for digital revolution. Through its Digital Dialogue Programme, the ECCB continues to explore, support and encourage Eastern Caribbean Currency Union (ECCU) member states to leverage the opportunities of digital technology and solutions.

The ECCB is a major partner and contributor of the Organisation of Eastern Caribbean States - Caribbean Digital Transformation Project.

The opportunities of a digital economy are boundless, however, consideration must be given to associated risks such as data and privacy breaches and cyber-attacks. FIs are encouraged to leverage the benefits of digital innovative solutions to include artificial intelligence, where greater efficiency, significant cost reduction, and improved customer experience can be realised while ensuring safety and security is embedded within the implemented systems.

Additional resources

https://www.fatfgafi.org/en/publications/Digitaltransformation/

https://www.eccb-centralbank.org/digital-dialogues

https://www.eccb-centralbank.org/digital-economy

Customer due diligence (CDD) measures involve identifying and verifying the identity of a customer. CDD measures could be enhanced or simplified. Simplified customer due diligence (simplified CDD) is a reduced level of CDD that a FI can apply to customers when the risk of money laundering (ML) and terrorist financing (TF) is deemed very "low". It however, requires an institution to apply the relevant components of CDD as outline in the Financial Action Task Force (FATF) Recommendation 10 - CDD. These include:

- Customer identification and verification;
- Beneficial owner identification and verification;
- Understanding the purpose and intended nature of the relationship; and
- Conducting ongoing monitoring.

As part of Recommendation 10, the FATF recommends that due diligence measures should be undertaken when:

- Establishing a business relationship;
- Suspicion is raised about ML or TF;
- Carrying out occasional transactions above the designated threshold; and
- The FI questions the adequacy of previously obtained customer identification data.

FIs are required to apply CDD measures, but should determine the extent of such measures utilising a risk-based approach; taking into consideration a country's ML/TF national risk assessment. An institutional ML/TF risk assessment should take into consideration the risk posed by its customers, countries or geographic areas with which they interact, products, services, and delivery channels. These variables may increase or decrease the potential ML/TF risk of a customer. The resulting customer risk rating guides the application of enhanced or simplified CDD. Recommendation 10 also provides the following examples of instances of lower risk and thus, where Simplified CDD may be applied:

- Public companies listed on a stock exchange and subject to disclosure requirements;
- A financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis;
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes; and
- A FI and designated non-financial business and profession (DNFBP) - where they are subject to requirements to combat ML and TF consistent with the FATF Recommendations.

The FATF emphasises that having a lower ML and TF risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions. Additionally, Simplified CDD measures are not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk is identified.

Source

1. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
2. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Financial-inclusion-cdd-2017.html

REGULATORY UPDATES

THE ECCB ISSUED DIRECTIVES AND ADVISORIES ON FINANCIAL CYBERCRIME

1

Supervisory analysis indicated that the use of FIs by cybercriminals, through the impersonation of account holders, were on the rise. Accordingly, in May 2023, the ECCB issued a directive on financial cybercrime to all licensed financial institutions (LFIs) in the ECCU member states where it had been named as AML/CFT Supervisory Authority. Where the ECCB was not named as Supervisory Authority, an advisory was issued.

LFIs were reminded of the requirement to ensure that their implemented systems and procedures are capable of adequately guarding against financial cybercrimes. They were reminded that they should be guided by the minimum requirements outlined in the Prudential Standard for Technology Risk Management for Institutions Licensed Under the Banking Act, 2015. In an effort to deter the growing trend of cyber-enabled fraud within the banking sector, LFIs were instructed to assess the risks posed, implement know your customer practices, empower and educate customers, and report all executed and attempted occurrences of fraudulent activity to the relevant authority.

WOLFSBERG GROUP UPDATED GUIDELINES AND BEST PRACTICES FOR ANTI-BRIBERY AND CORRUPTION PROGRAMMES

2

The Wolfsberg Group published its updated Anti-Bribery and Corruption (ABC) Compliance Programme Guidance on 17 April 2023. The 2023 guidance updated the 2017 version and was designed to promote a culture of ethical business practices and compliance with ABC legal and regulatory requirements. The guidance is a risk-based approach for the adequate development and implementation of compliance programmes to prevent, detect, and report acts of bribery and corruption and identifies areas of elevated risk. The guidance can help LFIs to mitigate bribery and corruption risks by utilising various elements. These include, but not limited to, an institution wide ABC policy, governance with roles and responsibilities and access to top management, periodic risk assessments to assess the nature and extent of the bribery and corruption risks, and training and awareness including the sharing of lessons learned from internal and external events for continuous evaluation of the compliance programme adequacy.

https://wolfsberg-group.org/news/39

FATF ADDED CROATIA, CAMEROON AND VIETNAM TO GRAY LIST, WHILE ISSUING WARNING TO JAMAICA AND BARBADOS

3

On 23 June 2023, the FATF added Cameroon, Croatia and Vietnam to its "*Jurisdictions under Increased Monitoring*" list, also known as the "*grey list*". When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring.

The FATF expressed concern that Barbados failed to complete its action plan, which fully expired in April 2022. The FATF strongly urged Barbados to swiftly demonstrate significant progress in completing its action plan by October 2023, or the FATF will consider next steps if there is insufficient progress.

The FATF, again, expressed concern that Jamaica failed to complete its action plan, which fully expired in January 2022. The FATF strongly urged Jamaica to swiftly demonstrate significant progress in completing its action plan by October 2023, or the FATF will consider next steps, which could include calling on its members and urging all jurisdictions to apply enhanced due diligence to business relations and transactions with the country.

https://www.fatf-gafi.org/en/publications/Fatfgeneral/Increased-monitoring-june-2023.html

OUTCOMES OF THE JUNE 2023 FATF PLENARY

4

The last plenary of the FATF, under the Singapore Presidency of T. Raja Kumar, took place over the period 21 to 23 June 2023. The following are the highlights:

- The suspension of the membership of the Russian Federation continued to stand. Following the statements issued in March 2022, the FATF reiterated that all jurisdictions should be vigilant to current and emerging risks from the circumvention of measures taken against the Russian Federation in order to protect the international financial system.

- FATF members agreed to publish the fourth targeted update on the implementation of the FATF Recommendations on virtual assets and virtual asset service providers. FATF members also advanced the work on preventing the misuse of non-profit organisations (NPOs) and agreed to release for public consultation, potential revisions to Recommendation 8 and the updated FATF Best Practices paper on combating the abuse of NPOs.

- The Plenary discussed potential enhancements to its Recommendations 4 and 38 to provide countries with stronger legal measures to freeze, seize and confiscate criminal property and property of corresponding value, including non-conviction based confiscation. The FATF expects to complete these projects in October 2023.

- FATF members agreed on new projects including a project to enhance ML investigations and prosecutions.

- The Plenary thanked outgoing Vice-President Elisa de Anda Madrazo of Mexico for her service, and welcomed Jeremy Weil of Canada, who will succeed her on 1 July 2023.

https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2023.html

5

SAINT VINCENT AND THE GRENADINES PASSED THE ANTI-TERRORISM (COMMENCEMENT & VALIDATION) BILL 2023 DURING SPECIAL SITTING OF THE HOUSE OF ASSEMBLY

The Anti-Terrorism (Date of Commencement and Validation) Bill, 2023 passed the committee stage without alterations on 1 June 2023, during a special session of the House of Assembly in Saint Vincent and the Grenadines. The Bill was taken through all phases during the special sitting, which also served as the final sitting in the 200-year-old Historic Court House Building.

Dr Honourable Ralph Gonsalves, Prime Minister and Minister of National Security, stated in opening debate on the Bill that the Anti-Terrorism Act 2023 was passed in the House of Assembly on 21 March 2023 and published in the Gazette as Act No. 5 of 2023. He noted, however, that while the Act was published in the gazette, it was not into effect at the time.

READ MORE

https://www.stvincenttimes.com/st-vincent-passes-anti-terrorism-bill-2023-during-special-sitting-of-parliament/

6

APPROVAL OF THE COMMONWEALTH OF DOMINICA'S 4TH ROUND MUTUAL EVALUATION REPORT

The Caribbean Financial Action Task Force's (CFATF) 56th Plenary approved the mutual evaluation report of the Commonwealth of Dominica, following discussions at both the CFATF Working Group on FATF Issues (WGFI) meeting and at Plenary. The report sets out the level of effectiveness of the country's AML/CFT system and its level of compliance with the FATF Recommendations. The completion of the post-Plenary Quality and Consistency process was pending.

READ MORE

CFATF 56th Plenary and Working Group Meetings Outcomes (cfatf-gafic.org)

GUIDANCE FOR EFFECTIVE TRANSACTION MONITORING

Transaction monitoring is "the process of monitoring transactions after their execution in order to identify unusual transactions including monitoring single transactions, as well as transaction flows".

It is a key control to mitigate ML/TF risk. The Bank for International Settlements notes that transaction monitoring is a particularly important aspect of FIs' due diligence, as it allows them to identify criminal activities and report those activities to the relevant authorities.

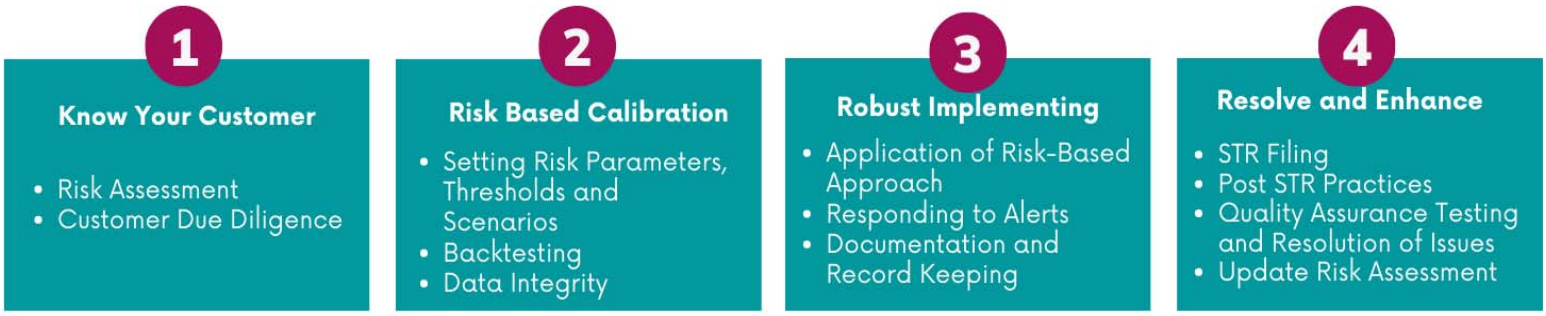
There are two (2) approaches to transaction monitoring:

1. Real time monitoring - this occurs as the transaction takes place and reduces the risk of breaching sanctions; and
2. Monitoring subsequent to the conduct of a transaction - which can be useful for identifying patterns and trends of criminal activities.

The ultimate goal of monitoring is to ensure that transactions are consistent with the FI's knowledge of the customer and to identify unusual activities for further investigation.

See **diagram 1** illustrating the transaction monitoring process chain extracted from the Monetary Authority of Singapore's – Guidance for Effective AML/CFT Transaction Monitoring Controls

Diagram 1 - Transaction Monitoring Process Chain



A risk-based approach to transaction monitoring

When implementing a transaction monitoring solution, FIs should:

- Establish internal policies - it is imperative that policies are implemented governing the oversight, review, and approval of the transaction monitoring processes, as well as the established parameters.

- Conduct a customer ML/TF risk assessment that is based on the customer's profile, products and services, geographies, delivery channels, nature of transactions and the frequency of transactions. This risk assessment would then guide transaction monitoring activities.

- Compare the customer's account/transaction history to their profile to identify patterns of suspicious activity or anomalies.

- Managing transaction alerts based on risk to ensure that unusual/suspicious activities are detected and actioned in an appropriate time.

- Investigative and, where applicable, report unusual transactions.

LFIs are reminded that effective transaction monitoring is centred on the understanding of its customers. This knowledge provides a basis for the implementation of relevant controls to assess customers' activities and behavioural patterns, which may pose risk to the LFI. It is therefore essential that LFIs maintain accurate and current customer information through the conducting of periodic reviews.

THE DEPARTMENT OF THE TREASURY'S DE-RISKING STRATEGY

A study by the United States (US) Department of Treasury found that de-risking poses a challenge to both public and private sector participants in providing responsible access to financial services, advancing US foreign policy and the centrality of the US financial system, and combatting illicit finance.

It was noted that the practice of "de-risking" was not in line with the risk-based approach that is attributed to the AML/CFT regulatory framework for US FIs under the Bank Secrecy Act and implementing regulations.

This is due to the fact that de-risking is used by FIs to terminate or restrict business relationships extensively with broad categories of clients rather than analysing and managing the risk of clients in a targeted manner.

The study focuses on three (3) categories of customers including small and medium-size Money Service Businesses, NPOs operating abroad in high-risk jurisdictions and Correspondent Banking Accounts with foreign FIs.

The result of the study revealed that the problem of "*de-risking*" was exaggerated for those institutions operating in financial environments characterised by high ML/TF risks. The study noted that the most important factor in de-risking was profitability, however, there were other factors that contribute to and/or exacerbated the effects of de-risking including AML/ CFT risks.

Accordingly, the effective solution to the issue of de-risking is a collaborative effort between private and public stakeholders, both domestically and internationally, finding ways to support the effort to address the adverse consequences of de-risking such as providing technical assistance abroad, and helping to ensure strong and consistent application of international standards to AML/CFT regulation and supervision. According to the study "*continued open engagement and dialogue, as well as commitment to help improve financial inclusion are essential to mitigate the causes of de-risking and to strengthen the AML/CFT regimes of the US and the rest of the world*".

The Department of the Treasury's De-Risking Strategy

ONCE A PEP ALWAYS A PEP?

INTERNATIONAL GUIDANCE ON THE TREATMENT OF PEPS

Assessments by the FATF and FATF styled bodies have revealed challenges with the effective implementation of the politically exposed person (PEP) requirements for competent authorities, FIs and DNFBPs worldwide. At the basic level, some FIs have struggled in collating a comprehensive list of PEPs due to their interpretation of the definition of a PEP.

The FATF defines a PEP as an individual who is or has been entrusted with a prominent public function.

Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing ML offences and related predicate offences including corruption and bribery, as well as conducting activity related to TF and Proliferation Financing (PF).

In February 2012, the FATF expanded the mandatory requirements to domestic PEPs and PEPs of international organisations, in line with Article 52 of the United Nations Convention against Corruption (UNCAC). Article 52 of the UNCAC defines PEPs as "*individuals who are, or have been, entrusted with prominent public functions and their family members and close associates*", and includes both domestic and foreign PEPs.

Determining whether customers or beneficial owners are PEPs and/or finding out who are their family members and close associates can be challenging, particularly when dealing with foreign PEPs for whom current information may not be readily available. The FATF notes that unlike law enforcement and supervisors, FIs have access to a valuable source of information: the customer.

They should utilise this rather than relying on third party providers. However, FIs will often need to utilise more than one sources of information to support CDD and/or to gather other information required by FATF Recommendation 12. Sources of information for the determination of PEPs, their family members and close associates include:

a) **Ensuring client CDD information is up-to-date** - existing customers sometimes become PEPs after they establish a business relationship with a FI. It is therefore essential that FIs monitor non-PEP accounts for a change in the PEP status, customer profile or account activity and update customer information.

b) **Employees** - training programmes need to address effective ways of determining whether customers are PEPs and to understand, assess and manage the potential risks associated with PEPs.

c) Internet and Media Searches

d) **Commercial Databases** - There are a variety of commercial databases available which may assist in the detection of PEPs. The use of these databases should however, never replace traditional CDD processes.

e) Government issued PEP-Lists

f) In-house databases and information sharing within financial groups or countries

g) **Asset Disclosure Systems** - countries may have asset disclosure systems in place that apply to those individuals that hold prominent public functions.

h) **Customer Self-Declarations** - self-declaration by a customer of their PEP status is known as a means of helping to determine whether that customer is a PEP.

i) **Information sharing by competent authorities.**

An area of concern for many LFIs is whether to apply enhanced due diligence (EDD) measures for PEPs who are no longer in office and by extension, their families and associates. Clarity on the time limits of a PEP status can be found in the FATF's Guidance on PEPs (2013). The guidance proposes that the language of Recommendation 12 is consistent with a possible open ended approach (that is, once a PEP – could always remain a PEP). Therefore, the handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits.

The risk based approach requires that FIs and DNFBPs assess the ML/TF risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors are:

1. The level of (informal) influence that the individual could still exercise;
2. The seniority of the position that the individual held as a PEP; or
3. Whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

The FATF guidance outlines measures applicable to the different types of PEPs, as follows:

1. Foreign PEPs are always considered high risk, and warrant implementing EDD measures.
2. Business relationships with domestic PEPs and international organisation PEPs that are determined to be high risk should be subject to EDD measures. In both circumstances, the following EDD measures apply:
    a. Senior management approval;
    b. Reasonable measures to establish the source of wealth and the source of funds; and
    c. Enhanced ongoing monitoring of the business relationship.
3. When a risk assessment established that a business relationship with a domestic/international organisation PEP does not present a higher risk, the PEP in question can be treated like any other normal customer. That is, the FI and DNFBP should apply normal customer due diligence measures and monitoring.

Source: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html#:~:text=FATF%20Guidance%3A%20Politically%20Exposed%20Persons%20(Rec%2012%20and%2022)&text=A%20politically%20exposed%20person%20(PEP,such%20as%20corruption%20or%20bribery

SALE OF FAKE VIRTUAL ASSETS IN AZERBAIJAN

A typology by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) in its 2023 publication – Money Laundering and Terrorist Financing Risks in The World of Virtual Assets

Persons (citizens of a foreign country) who previously registered a company in a foreign country, which operates in the "*emission of virtual currency*" field, registered an advertising company in Azerbaijan.

The Azerbaijan company promoted a fake cryptocurrency stating that soon this cryptocurrency ("XYZ Coin") would be traded on various international cryptocurrency exchange platforms. The perpetrators were able to collect large sums of money from citizens who were promised exaggerated high revenues for investing in XYZ Coin. Three (3) forms of earning opportunities were proposed to those who acquired XYZ Coin:

1) Dividend payment corresponding to the funds invested for the purchase of XYZ Coin (after a period of time);
2) Commission payment for encouraging other people to invest in XYZ Coin; and
3) Payment of high profits after the future listing of XYZ Coin on a foreign exchange.

Criminals artificially increased the price of XYZ Coin every few months to increase their illegal income, stating that the price increase was owed to the listing of XYZ Coin on a foreign exchange. The alleged criminals, in order to artificially reduce the value of persons' investment in XYZ Coin for their own benefit, gave a discount to the persons who bought the coin on the website XYZCoin.com, offering to exchange two (2) XYZ Coins on XYZCoin.com for one (1) XYZ Coin placed on the stock exchange.

Funds transferred to the cards of the Azerbaijan company for the purpose of purchasing XYZ Coin amounted to several million currency units, two-thirds (2/3) of which consisted of payments made through payment terminals. The investigation revealed that the company was not listed on any cryptocurrency exchange platform. Additionally, the declared cryptocurrency was just a pseudo-token where the transfer of the relevant token to another individual on the exchange was described as the sale process of virtual currency to network members.

Source: Page 39, https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4

Have you read the previous issues of the AML/CFT Newsletter?

Download your copy from the Publications section of the ECCB Website at https://www.eccb-centralbank.org/publications/other-publications

Thank you!

The Eastern Caribbean Central Bank

P O Box 89
Basseterre
St Kitts and Nevis
West Indies

Tel: (869) 565-2537
Fax: (869) 565-9562

The ECCB welcomes your feedback and suggestions towards improving the utility of this newsletter to your institution. Please make your submissions to:
Email: AMLSupervisoryUnit@eccb-centralbank.org

@ECCBConnects

https://www.eccb-centralbank.org/

@ECCBConnects

Eastern Caribbean Central Bank