AML/CFT NEWSLETTER

ISSUE 7 SEPTEMBER 2022

SUSPICIOUS ACTIVITY INVESTIGATION AND REPORTING - BEST PRACTICES FOR LFIs

By the Financial Intelligence Authority- Saint Lucia

Financial crime poses a threat to the financial community and has become increasingly harder to detect. Criminals assisted by the advancements in technology utilise sophisticated schemes to launder their ill-gotten gains. This increase in financial crime exposes financial institutions to numerous risks which has resulted in the implementation of more robust Anti-Money Laundering, Counter Terrorist Financing and Proliferation (AML/CFT/CPF) compliance programs.

An essential component of a robust AML/CFT/CPF compliance program is its capability to identify and report suspicious activities. Financial institutions are required by law to have adequate policies, procedures and controls in place to detect, investigate and report suspicious activities to the relevant authority.

THIS ISSUE'S CONTENT

They are obligated to analyse transaction details, including the nature and purpose of the transaction which may indicate potential money laundering (ML) or other illegal activities.

This duty to investigate and report suspicious activity, is a direct consequence of the Financial Action Task Force (FATF) Recommendation 20 - Reporting of Suspicious Transactions, which states *"if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing (TF), it should be required by law, to report promptly its suspicions to the Financial Intelligence Unit"*.

Suspicious activities are transactions which appears inconsistent with a customer's expected business activity, have no reasonable economic justification, seem illegal or are designed to evade the local anti-money laundering laws. Financial institutions knowledge of their customers and customer transactions places them in a vital position to report crucial information to law enforcement.

The reporting of suspicious activity takes place via the submission of a Suspicious Activity Report (SAR). A SAR is a document completed by a financial institution, within a stipulated timeframe and in accordance with their regulatory requirements. SARs enable law enforcement agencies to discover and prosecute financial crimes and other illegal endeavours. They provide law enforcement with opportunities to detect and analyse emerging trends and patterns across a broad spectrum of personal and organized crimes. It is imperative to note, however, that the reporting of suspicious activity does not equate to a criminal liability or a breach of confidentiality under banking legislation or any similar law for the filing institution and its employees.

A SAR is an effective tool in the fight against ML and organized crime once correctly completed.

The information gathered from SARs help initiate investigations, provide intelligence, and ultimately assist with safeguarding the integrity of the financial sector. A well-written SAR should be self-explanatory, as the receiver does not possess intimate knowledge of the transaction or customer. As such, SARs should always be written with law enforcement in mind.

A well-written SAR includes three (3) fundamental components:

1. An introduction;
2. A body; and
3. A conclusion.

The Introduction

The purpose of the introduction is to provide law enforcement and the analyst with quick responses to the following questions:

i. What is the activity?
ii. Why is it suspicious?
iii. Who is involved?
iv. What is the total amount involved?
v. What is the time period of the activity?
vi. What accounts are involved?
vii. How was the transaction facilitated?

It is prudent to include simple answers to these questions in the introduction, as the intention is to provide a synopsis for filing the SAR. A short explanation will suffice; the key is to keep the introduction simple.

The Body

The body of the SAR is an accurate, thorough and complete narrative detailing the particulars for the suspicion. This is the part of the SAR where financial institutions provide:

- ***Details about the suspect***- full name and alias, identification documents, nationality, occupation, address, all related accounts etc.
- ***Mechanisms utilised to facilitate the suspected transactions***- wire transfer, cheques, complex structures, shell companies, structuring, triggers by adverse media reports or regulatory requests.

- ***Dates and periods of the suspicious activity including when the financial institution identified the activity.***
- ***Locations associated with the suspicious activity***- details of the branches involved as well as any other financial institutions utilised in the scheme.
- ***Details of why the activity or transaction is unusual***- transactions are much larger or more frequent than usual, transactions are from a high-risk country or region, or from a person or entity listed on a sanctions list.

The information included in the body of a SAR is solely to report the known or suspected violations observed by the financial institution and does not need to make a connection to the underlying predicate offense.

It is the responsibility of law enforcement, to key together the pieces of information and to connect the SAR with a predicate offense.

The Conclusion

The conclusion summarises the suspicious activity and should help law enforcement understand how the financial institution arrived at the decision and the factors that contributed to the determination of the suspicion.

Equally important to filling an SAR, is the significant measures taken by financial institutions to ensure this information remains confidential and that the subjects of the SARs are not tipped-off. Tipping-off occurs when a person discloses to another person, information which is likely to prejudice an investigation. This is a criminal offence and the consequences can impede the effective functioning of the reporting entity.

Additionally, the decision not to file an SAR is of equal importance as the decision to file an SAR. The final decision not to file, should be documented and supported by the reasoning that was used to make the determination. Financial institutions should also implement policies governing the non-filing of SARs.

The quality of the SARs filed by financial institutions alternately provides insight to regulators on the comprehensiveness of their AML/CFT/CPF programs, specifically their customer due diligence, ongoing monitoring and record keeping policies and procedures. Financial institutions must supplement the SAR narrative with the necessary supporting documentation. Supporting documentation may include transaction records, any account information, e-mail messages and other correspondences or any other information that will assist law enforcement.

REGULATORY UPDATES

Dominica enacts Virtual Asset Business Legislation

The Government of the Commonwealth of Dominica (Dominica) passed a Virtual Asset Business legislation in parliament on 30 May 2022. The Virtual Asset Business Bill was drafted with the assistance of the Eastern Caribbean Central Bank (ECCB) with the intention of harmonising legislation across all member states of the Eastern Caribbean Currency Union (ECCU).

The Act will provide for the registration and supervision of any person or business involved in the virtual asset business, established before or after the commencement of the legislation.

It provides for the Financial Services Unit of the Ministry of Finance to be responsible for the oversight of virtual asset businesses, except in the case of virtual assets that are considered investments products or services. Virtual assets considered as investments will be regulated by the Eastern Caribbean Securities Regulatory Commission under the Securities Act.

Dominica joins St Kitts and Nevis, and Antigua and Barbuda in the nine-member Organization of Eastern Caribbean States that have passed similar legislation.

READ MORE PARLIAMENT PASSES VIRTUAL ASSET BUSINESS ACT - GIS Dominica (news.gov.dm)

FinCEN Published Final Beneficial Ownership Rule

The United States Financial Intelligence Unit directed corporations, limited liability companies and a host of other legal entities in a final rule on 27 September 2022 to begin disclosing their beneficial owners to the Federal Government, commencing January 2024.

Entities created or registered before 1 January 2024 will have one (1) year to submit details on their owners to the Treasury Department's Financial Crimes Enforcement Network (FinCen), while entities that are registered or came into existence after that date, will have one (1) month to file their initial disclosures to the bureau.

All entities will then have one (1) month to notify FinCEN of any changes in their ownership information, according to the final rule.

READ MORE https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-beneficial-ownership-reporting-support-law-enforcement

THE ECCB AML/CFT MENTORSHIP PROGRAMME CONTINUED IN THREE ECCU TERRITORIES

The ECCB, through the provision of technical support, continued to assist ECCU member countries in the conduct of risk based AML/CFT/CPF examinations. During the quarter July – September 2022 the AML/CFT Mentorship Program continued in Saint Lucia, Saint Christopher (Saint Kitts) and Nevis, and Saint Vincent and the Grenadines.

This was made possible through the Caribbean Development Bank's (CDB) technical assistance project towards "Improving Integrity and Financial Transparency of the Eastern Caribbean Currency Union". The project aims to harmonise the approach to AML/CFT/CPF supervision across the various ECCU jurisdictions, in keeping with international best practices.

As a part of the preparations for the execution of the examination, the ECCB facilitated governance training for the participating supervisory and regulatory bodies. The training covered the five (5) pillar approach to assessing AML/CFT/CPF governance at licensed financial institutions (LFIs).

Representatives of the ECCB with Examiners from the Financial Intelligence Authority- Saint Lucia

Representative of the ECCB with Financial Inspectors from the Financial Services Regulatory Commission – Saint Kitts

Representatives of the ECCB with Examiners from the Financial Services Authority- Saint Vincent and the Grenadines

Mr. Jimmy Black
Examiner II
Financial Services Regulatory Commission, Saint Vincent and the Grenadines

"The hands on component of the mentorship program was an extremely effective tool to participants in St Vincent and the Grenadines. The experience gained will definitely strengthen our AML/CFT/CPF Supervisory Framework".

LFIs IN THE COMMINICA OF DOMINICA RECEIVED RISK ASSESSMENT TRAINING

The Commonwealth of Dominica's Fourth Round of Mutual Evaluations (MER) was schedule for the period 15 to 26 August 2022. To assist LFIs with their preparations for the MER, on 12 August 2022, the ECCB conducted a training session with LFIs in the territory. The training covered key topics including but not limited to:

- What is a national risk assessment?;
- Financial Action Task Force (FATF) Recommendation 1 - Assessing risks and applying a risk-based approach; and
- The ECCB's Banking Sectorial Risk Assessment.

FATF Recommendation 1 requires countries to identify, assess and understand their ML/TF/ proliferation financing (PF) risks. This forms a critical component of the implementation and development of an AML/CFT/CPF regime. The results of a national risk assessment assists in the prioritization and efficient allocation of resources through the application of a risk- based approach.

MANAGING THE RISK ASSOCIATED WITH HIGH RISK PRODUCTS AND SERVICES

Understanding and addressing the potential ML/TF/PF risks associated with customers and transactions is critical to effectively managing the continuing threat of financial crime through financial institutions.

High risks products and services are utilised in various sectors. While they may be used when conducting legitimate business, some aspects of their nature may make them susceptible to ML, TF, or PF. Common examples of inherently high risk products and services include wire transfers, chequing accounts, citizenship by investment related services and private banking. They may be misused by money launderers to legitimize their illicit proceeds or used by terrorists and proliferation financiers to facilitate crimes. To make their transactions indistinguishable from legitimate transactions, criminals become very creative aimed at circumventing the internal controls implemented by financial institutions. Therefore, it may be difficult, at times impossible, for an institution to distinguish between legal and illegal transactions, even in the presence of an effective and reasonably designed compliance programmes.

An effective risk-based framework which facilitates the identification of potential ML, TF and PF risks associated with customers and transactions, will allow a financial institution to focus on customers and transactions deemed to pose a heightened level of risk and implement adequate mitigating controls.

Some steps institutions can adopt to manage the risks associated with high risk products and services include:

1. **Adopting a Risk-based Approach (RBA) to AML/CFT/CPF:** this means that financial institutions, are expected to identify, assess and understand the ML/TF/PF risks to which they are exposed and take AML/CFT/CPF measures commensurate to those risks in order to mitigate them effectively. This include the way institutions allocate their compliance resources, organise their system of internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF/PF.

2. **Risk assessment:** this is a critical component of the RBA. The threat of ML/TF/PF can be managed effectively and efficiently by understanding and addressing the potential risks posed by customers and their transactions. A risk assessment need not be complex but should be commensurate with the nature and size of the institution's business. The most commonly used risk criteria are country/geography risk, customer risk, product and service risk, and delivery channel risk.

3. **Risk mitigation**: define actions to mitigate risk by focusing on customer due diligence (CDD), ongoing monitoring and reporting frameworks. An assessment of ML/TF/PF risks will result in the application of appropriate due diligence when entering into a relationship with a customer, and ongoing due diligence and monitoring of transactions throughout the business relationship.

   A **CDD** framework should assist LFIs in understanding who their customers, are by requiring them to gather information on the nature of their business, for example, what they do and why they require banking services. Based on a holistic view of the information obtained during onboarding, LFIs are required to complete a customer risk profile. This will influence the level and type of ongoing monitoring and support the entity's decision whether to enter into, continue or terminate the business relationship.

   Ongoing monitoring - for some customers, potential risks can only be identified upon commencement of the business relationship and during the ongoing monitoring process.

Ongoing monitoring involves scrutiny of transactions to determine whether they are consistent with the LFI's knowledge of the customer and the nature and purpose of the business relationship. This involves identifying changes to the customer profile, for example, their use of certain products and services, the account activity, and the volume and value of transactions. It also requires keeping the customer profile up to date, which may require the application of additional or enhanced CDD measures. Transaction Monitoring is an essential component in identifying transactions that are unusual and potentially suspicious. LFIs must adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher risk situations, while LFIs may decide to reduce the frequency and intensity of monitoring where the risks are lower.

Reporting: FATF Recommendation 20 and national AML/CFT/CPF laws require LFIs to report suspicion promptly to the relevant Financial Intelligence Unit where it suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to TF or PF.

LFIs should have the ability to flag unusual movement of transactions or funds for further analysis. It is recommended that institutions have appropriate case management systems, so that such funds or transactions are scrutinized in a timely manner and a determination made as to whether the funds or transaction are unusual or suspicious.

4. Implementation and enforcement of a system of internal controls

Internal controls are critical for the effective implementation of policies and processes to mitigate AML/CFT/CPF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT/CPF is clearly allocated, controls to monitor the integrity of staff, compliance and controls to test the overall effectiveness of the LFI's policies and processes in identifying, assessing and monitoring risks.

WORLD BANK AML/CFT RISK-BASED SUPERVISION TOOL, MODULE 5 - BANKING SECTOR DIALOGUE AND COLLABORATION WORKSHOP

The AML/CFT Risk-based Supervision, Banking Sector Dialogue and Collaboration Workshop (Module 5) is a component of an assistance program provided by the World Bank, with funding from the European Union to the member countries of the ECCU. It provides a toolkit to enhance supervisory capabilities and implement a risk-based approach. The program is currently being administrated by the ECCB.

Module 5 was aimed at strengthening the dialogue and cooperation between the supervisory agencies and reporting entities. The session also sought to clarify the regulatory expectations and the guidance needs of the private sector.

The workshop provided supervisory authorities with tools to guide, lead and provide feedback to the private sector towards an effective risk-sensitive implementation of AML/CFT measures. It also provided an opportunity to identify the challenges faced by private sector entities related to compliance, thus allowing authorities and private sector entities to reach joint solutions.

The Dialogue and Collaboration Workshop was held in three (3) sessions, with the first plenary session taking place in November 2021, the second session in January 2022 and the third session on 18 July 2022.

EFFECTIVE AML/CFT/CPF SUPERVISION THROUGH COLLABORATION

Representatives of the ECCB with Examiners from the Office of National Drug and Money Laundering Control Policy- Antigua and Barbuda

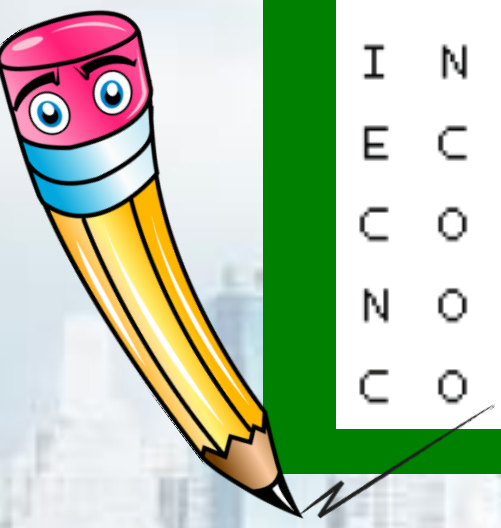
Building and sustaining meaningful and effective relationships as AML/CFT/CPF supervisors are essential in strengthening the AML/CFT/CPF landscape within the ECCU.

Enhanced collaboration between AML/CFT /CPF supervisors can improve the effectiveness of supervision, increase alignment of supervisory measures and foster a safer financial sector.

In August 2022 the ECCB and Examiners within the Office of National Drug and Money Laundering Control Policy (ONDCP) performed joint thematic reviews of licensed financial institutions in Antigua and Barbuda. The examinations focused on AML/CFT/CPF governance and ongoing monitoring.

AML WORD SEARCH

S	L	N	N	T	R	J	W	F	M	C	R	Y	E	D
E	C	N	A	N	R	E	V	O	G	Y	E	C	R	E
S	H	N	I	S	L	L	N	H	G	B	G	N	A	T
Z	E	E	O	S	H	I	U	N	Z	E	U	E	W	E
J	S	I	J	I	T	U	I	S	U	R	L	R	M	C
N	H	Q	C	O	T	N	E	N	X	S	A	A	O	T
W	R	P	R	I	I	A	T	D	Q	E	T	P	S	I
K	B	I	Z	A	L	C	R	V	J	C	I	S	N	O
Q	N	M	R	X	O	O	X	E	A	U	O	N	A	N
G	K	T	G	K	W	Q	P	B	F	R	N	A	R	A
I	N	T	E	G	R	I	T	Y	D	I	S	R	G	C
E	C	N	A	I	L	P	M	O	C	T	L	T	Z	K
C	O	R	R	U	P	T	I	O	N	Y	D	O	C	N
N	O	I	T	N	E	V	E	R	P	U	S	B	R	Z
C	O	O	P	E	R	A	T	I	O	N	T	P	E	P



Compliance
Cybersecurity
Integrity
Prevention
Regulations

Cooperation
Detection
Monitoring
Proliferation
Training

Corruption
Governance
Policies
Ransomware
Transparency

SOCIAL ENGINEERING: THE HUMAN ELEMENT OF CYBERSECURITY

Historically, user action and or inaction have often been a factor in cybersecurity issues.

Social engineering is the art of human manipulation.

Cybercriminals use varying techniques that rely heavily on human interaction. They attempt to convince potential victims to do something their victim would usually not do. This may include tricking users into providing sensitive information or access, and performing operations to increase the success rate of cyberattacks.

Social engineering attacks often occur in a number of phases. Cybercriminals prepare by conducting reconnaissance on intended victims to gather necessary background information and then presents the target with seemingly credible information or requests. This is ultimately to gain the victim's trust and provide stimuli for subsequent actions.

Some of the common attack methods include phishing and spear phishing emails, compromised websites, vishing (voice calls) and real-world baiting. The information or access gained from the initial attack is often leveraged to further exploit the victim through data theft, data exposure, ransomware, extortion and denial of access.

Social engineering is one of the most common and effective ways an attacker can gain access to sensitive information.

Statistics on social engineering attacks indicate that over recent years it has grown significantly in volume and complexity. Today, a high percentage of successful breaches is either initiated via a social engineering attack or included a social engineering attack at some stage. As a result, it is important that individuals and organisations equip themselves with sufficient knowledge, in addition to technical controls to mitigate the risk. User awareness and the adoption of a culture of cybersecurity are critical to mitigating social engineering attacks. This is because the intention of the deception is to target humans as the

perceived weakest link to bypass technical controls.

At the individual level, do you know your digital footprint?

This is the trail of information you leave behind whenever using the internet. For example, posting on social media, subscribing to a newsletter, leaving an online review, or shopping online. Digital footprints can be *'active'* or *'passive'* and they do matter because they are often leveraged by cybercriminals for exploitation purposes. These can include phishing for account access or creating false identities based on your data.

Vigilance is key when handling each individual email and unsolicited interaction for potentially malicious artefact and intent. As a general rule of thumb, the following will help to improve vigilance in relation to social engineering attacks:

- Do not open emails and attachments from suspicious sources. Emails from known sources can also be potentially dangerous as attackers may sometimes leverage your peers and known associates to attack you. For this reason, try to be an advocate for cybersecurity by sharing your knowledge on secure behaviour with your family, peers and associates.
- Do not be a clicker. Every time you click on a link or open an attachment in an email, be sure it is a deliberate action based on the determination that the link or attachment are safe to access.
- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise.
- Always keep your personal antivirus/anti-malware software updated. It is important to turn on automatic updates and periodically check that all updates are being successfully applied and to scan your system for possible infections.

At the organisation level, the aforementioned user awareness and building the culture of cybersecurity across the organisation are equally significant.

Continual assessment of the human factor, using real world simulations is important for positive reinforcement of the security awareness training. This, along with practical policies and procedures supported by tools to guide prevention, detection, reporting, investigation and remediation of cyber incidents can go a long way towards mitigating social engineering attacks.

MONEY LAUNDERING TYPOLOGY

Fraud charges brought against David Ames

The Serious Fraud Office (SFO) in the United Kingdom convicted David Ames on two (2) counts of fraud by abuse of position on 3 August 2022. Ames was the individual behind a £226 million fraud involving celebrity-endorsed luxury resorts in the Caribbean.

The investigation revealed that Ames deceived over 8,000 UK investors in the Harlequin Group, a hotel and resorts development venture. Victims were led to believe they had a secure investment in property whereas, in reality, Harlequin Group was never operating as promised.

Ames made publicity a key priority, promising celebrity-sponsored tennis, golf and football academies with marketing videos in which he personally explains his vision for the resorts. Predicting major tourism development opportunities, he even secured the endorsement of politicians in the region.

The investigation revealed that by the time it went into administration in 2013, Harlequin had sold around 9,000 property units to investors, with less than 200 ever actually being constructed. Ames enriched himself and his family by £6.2 million. The Harlequin companies were family businesses, employing at certain times both David Ames' wife and his son, who was paid £10,000 per month. Ames had been temporarily barred from serving as a company director due to a previous bankruptcy and therefore styled himself as the "Chairman of Harlequin".

A thorough enhanced due diligence check of David Ames would have revealed that Ames had a history of bankruptcies and was barred from being a director. The use of his family in the business and paying them exorbitant salaries were all red flags that could have alerted to suspicious activities in this venture.

https://www.sfo.gov.uk/2022/08/03/fraudulent-caribbean-resorts-owner-convicted-after-sfo-investigation/#:~:text=David%20Ames%2C%2070%2C%20was%20today%20found%20guilty%20by,Harlequin%20Group%2C%20a%20hotel%20and%20resorts%20development%20venture.investigation/#:~:text=David%20Ames%2C%2070%2C%20was%20today%20found%20guilty%20by,Harlequin%20Group%2C%20a%20hotel%20and%20resorts%20development%20venture.

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

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

Thank you!

The Eastern Caribbean Central Bank

P O Box 89
Basseterre
St Kitts and Nevis
West Indies

Tel: (869) 465-2537
Fax: (869) 465-9562

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