AML/CFT NEWSLETTER

ISSUE 5 MARCH 2022

THE CFATF 4TH ROUND MUTUAL EVALUATION PROCESS

The Antigua and Barbuda Experience

By Derek Benjamin – Manager, Financial Compliance Unit, Office of National Drug and Money Laundering Control Policy, Antigua and Barbuda

The Caribbean Financial Action Task Force (CFATF) is a regional organisation representing a membership of twenty-six (26) Caribbean, Central and South American states. The CFATF is an associate member of the Financial Action Task Force (FATF), the international organisation which sets the standards to promote the effective implementation of legal, regulatory and operational measures for combatting money laundering (ML), terrorism financing (TF), proliferation financing (PF) and other related threats to the integrity of the international financial systems. All eight (8) member countries of the Eastern Caribbean Currency Union (ECCU) are members of the CFATF. As a member of the CFATF, member countries agree to implement common countermeasures to combat money laundering and the financing of terrorism (The FATF Recommendations).

THIS ISSUE'S CONTENT

The implementation of these recommendations/ countermeasures is assessed through an ongoing program of 'mutual evaluation', a peer-to-peer assessment of member states, managed by the CFATF Secretariat.

The CFATF 4th round of Mutual Evaluations has adopted complementary approaches for assessing technical compliance with the FATF Recommendations and for assessing whether and how the AML/CFT system is effective.

The Mutual Evaluation (MEV) process is guided by the FATF Methodology which provides the benchmarks for assessing a country's compliance with the FATF Recommendations. This methodology sets out the criteria for assessing levels of technical compliance with each of the FATF Recommendations and the outcomes, indicators, data and other factors used to assess the effectiveness of the implementation of the FATF Recommendations.

The technical compliance assessment addresses the specific requirements of the FATF Recommendations, principally as they relate to the country's legislative and institutional framework and the powers and procedures of the competent (supervisory, regulatory and law enforcement) authorities. Countries are required to provide the modality adopted – Laws, Regulations, Guidelines or Directives – which provide an enforceable measure to give legal effect to the FATF Recommendations.

The effectiveness assessment is a demonstration of "Practice what you preach" or "Words in action". It differs from the assessment of technical compliance, as it seeks to assess the adequacy of the implementation of the country's legislative framework in meeting the FATF 40 Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are key to a robust AML/CFT system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional frameworks are producing meaningful results.

Although the assessments of both technical compliance and effectiveness are measured along with different standards – technical compliance is based on the FATF Recommendations and effectiveness based on the eleven (11) Immediate Outcomes (IO), there is a cascading link between both assessments.

Countries must recognise that the development of effective countermeasures to combat ML, TF and PF are not contingent on the efforts of any one agency or authority.

It requires the full participation of several stakeholders – policymakers, regulators, supervisors, self-regulatory bodies, law enforcement agencies and all financial sectors/institutions. This effort should be sufficiently coordinated via a national framework or overarching body.

The Mutual Evaluation is an intricate process which allows for interactive synergy between the assessment team and the assessed country; the result being a "mutually acceptable report".

Antigua and Barbuda's 4th Round Mutual Evaluation Assessment was conducted over a period of nineteen (19) months.

It commenced with the preparation and submission of the country's Technical Compliance Questionnaire (TCQ) in December 2016, followed by the submission of the Effectiveness Assessment annex in February 2017.

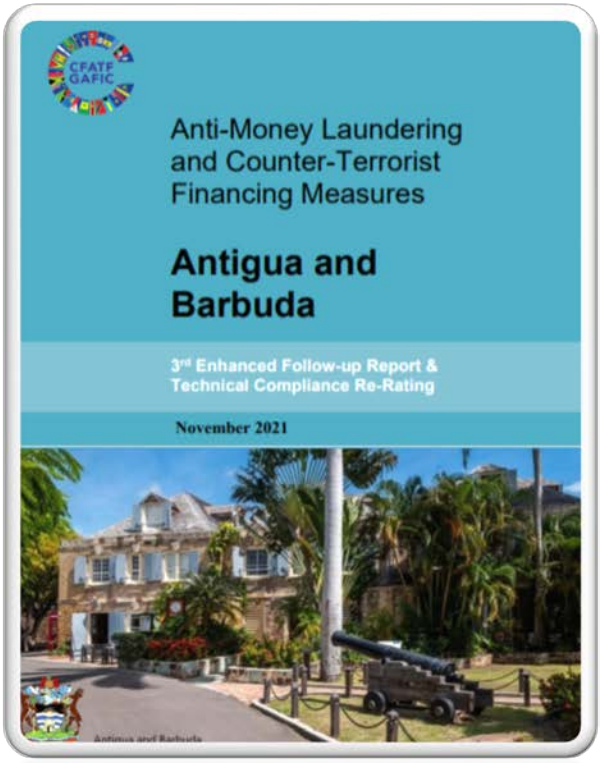
This was followed by the onsite visit, 5th – 16th June 2017 and thereafter the receipt, review and response to the 1st, 2nd and 3rd drafts of the Mutual Evaluation Report (MER). Between the time of reviewing the 2nd draft and prior to the issuance of the 3rd draft, the CFATF assessment team and country representatives met face-to-face for further interventions, before the report was presented to the CFATF Working Group on FATF Matters (WGFI) and the CFATF Plenary in May 2018 for a final arbitration, Plenary debate and adoption for submission to the FATF Plenary. Final ratification and publication were in July 2018.

The preparation for the MEV, along with the ensuing reviews and responses to the MER edits, required the coordinated participation of several national stakeholders – supervisory authority, regulatory authorities, law enforcement and legal authorities.

Antigua and Barbuda recognised that it was extremely important that all stakeholders were cognisant of their roles within the national AML/CFT/CPF framework.

Many elements relating to the implementation of the FATF Recommendations were not exclusively addressed in AML/CFT/CPF legislation. It was therefore necessary that there was a collective harnessing of the national interagency intellectual pool, so that there was a complete representation of the national framework.

Antigua and Barbuda's preparations included weekly meetings of relevant authorities - Police, Defence Force, Customs, Intellectual Property, Ministry of Finance, Ministry of Legal Affairs, Director of Public Prosecution, Financial Services Regulatory Commission, and the Office of National Drug and Money Laundering Control Policy under the chairmanship of the Prime Minister of Antigua and Barbuda. There were also several meetings with the financial sector. The resulting outcome being, Antigua and Barbuda receiving 32 out of 40 Recommendations rated Compliant or Largely Compliant, along with 8 Immediate Outcomes rated Moderate and 3 rated Low. This however was not the end of the evaluation process, as the country was required to address and rectify the shortcomings identified in the report.



All countries are subject to post-assessment monitoring – the Follow-Up Report (FUR) process. This includes scheduled reporting on improvements made towards addressing identified deficiencies, a demonstrated commitment to address all shortcomings or in worst-case scenarios, the issuing by FATF of a public warning against a country that makes insufficient progress towards addressing key deficiencies.

In addition to addressing MER deficiencies (Recommendations rated Partially Compliant or Non-Compliant), countries are required to ensure that they adequately address any changes to the FATF Recommendations that may have been previously rated Compliant or Largely Compliant.

The Follow-Up process for CFATF 4th Round MEV focuses on addressing deficiencies identified in relation to technical compliance. The 5th Round MEV will focus on effectiveness and the eleven immediate outcomes.

REGULATORY UPDATES

ECCB NAMED AS AML/CFT/CPF SUPERVISORY AUTHORITY IN SAINT LUCIA

In November 2021, Saint Lucia amended its Anti- Money Laundering (Prevention) Act, Cap 12.20 (MLPA) to name the Eastern Caribbean Central Bank (ECCB) as the AML/CFT/CPF Supervisor for licensed financial institutions under the Banking Act 2015.

Accordingly, Section 5 of the Money Laundering (Prevention) (Amendment) Act No. 16 of 2021, inserts immediately after Part 2, of the MLPA - "PART 2A SUPERVISION OF A LICENSED FINANCIAL INSTITUTION.

Section 14B (1) of the MLPA states: *"For the purposes of this Act, the Central Bank is, without limiting the functions of the Authority under this Act, responsible for the supervision of a licensed financial institution in relation to money laundering, terrorist financing and proliferation financing*".

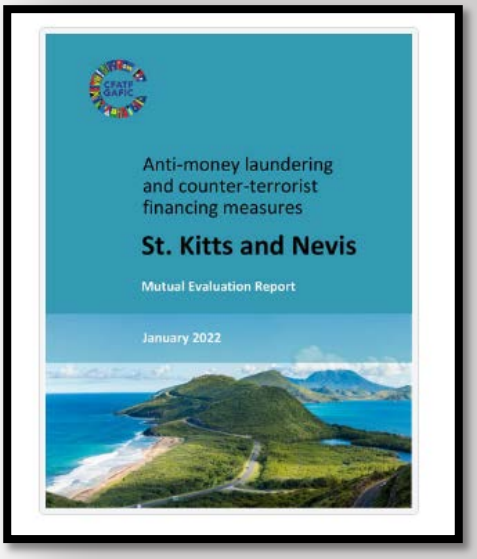
https://www.slufia.com/p/legislation

PROPOSAL TO ADD THE CAYMAN ISLANDS TO THE EUROPEAN UNION'S ANTI-MONEY LAUNDERING BLACKLIST

At its February 2021 plenary, the FATF concluded that Cayman Islands had satisfied 60 of the 63 recommendations in the 2019 Mutual Evaluation Report and should be placed on the FATF Ongoing Monitoring List. In October 2021, the FATF concluded that Cayman was making positive progress in satisfying the final outstanding recommendations arising from the effectiveness assessment and the country was either 'compliant' or 'largely compliant' with all 40 FATF technical recommendations.

Notwithstanding, on 21 February 2022, following the European Commission's proposal in January 2022, a Commission Delegated Regulation was published, which placed the Cayman Islands on the European Union's AML 'blacklist', along with eight (8) other jurisdictions, including Haiti.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0229&qid=1645520532786&from=en



4TH ROUND MUTUAL EVALUATION REPORT OF ST. KITTS AND NEVIS PUBLISHED

The CFATF Plenary held virtually in December 2021, adopted the Mutual Evaluation Report of St. Kitts and Nevis.

The report presents information on the level of compliance with the FATF 40 Recommendations, the level of effectiveness of the country's AML/CFT system and provides recommendations on how the system could be strengthened.

https://www.cfatf-gafic.org/home-test/english-documents/4th-round-meval-reports/17358-st-kitts-and-nevis-4th-round-mer

NOTICE TO LICENSED FINANCIAL INSTITUTIONS
THE ECCB INCREASES FOCUS ON PROLIFERATION FINANCING COMPLIANCE

In October 2020, the FATF revised Recommendations 1 and 2 and their Interpretive Notes, as part of its response actions to the threat of illicit proliferation of weapons of mass destruction. Recommendation 1 requires countries, financial institutions, designated non-financial businesses and professionals and virtual assets providers to identify, assess, and understand the proliferation financing (PF) risks for the country and to take action to mitigate these risks.

In June 2021, the FATF released guidelines to assist countries and private sector entities in effectively implementing the FATFs requirement to identify, assess, understand and mitigate their PF risks. This was to further support the revised guidelines issued in February 2018, providing specific measures that give effect to and implement United Nations Security Council Resolution 1540 (2004) and its successor resolutions, specifically on targeted financial sanctions to counter proliferation financing.

In that regard, effective January 2022, the ECCB increased its focus on PF risk and has consequently expanded its examination scope to include the assessment of entities' PF risk management framework. Licensed Financial Institutions (LFIs) are therefore required to take measures to assess their existing controls with a view to strengthening measures to identify, understand and assess PF risks and implement adequate controls to mitigate these risks.

The financing of weapons of mass destruction can have catastrophic impact to include loss of lives and financial instability. Taking action to support the fight against proliferation of weapons of mass destruction should therefore be a priority for every financial institution.

ELEMENTS OF A STRONG AML/CFT/CPF GOVERNANCE PROGRAM

The ECCB has adopted a risk based supervisory approach to AML/CFT/CPF, premised on the concepts and principles considered by the FATF and the Basel Core Principles. The Risk Based Approach (RBA) to AML/CFT/CPF complements the ECCB's approved prudential Risk Based Supervision (RBS) Framework for Licensed Financial Institutions.

The RBA for AML/CFT/CPF Governance recognises that a strong governance structure is critical to the success of the AML/CFT/CPF program and as such, the Board of Directors (the board) must provide for a framework of effective corporate governance with the support of senior officers. The board and senior officers are primarily responsible and ultimately accountable for the LFIs' compliance with applicable AML/CFT/CPF legislation and supervisory guidance. In this regard, the ECCB has implemented its five (5) pillar approach to assessing AML/CFT/CPF Governance at LFIs.

1

AML/CFT/CPF Risk Management Framework- LFIs must develop and implement a risk framework for the identification, measurement, reporting and monitoring of ML/TF/PF risks. LFIs must have a clear understanding of ML/TF/PF risks to which the institution may be exposed and implement measures to mitigate these risks. These measures include:

- A ML/TF/PF risk assessment based on customers, products, services, delivery channels and geographies;
- Board approved policies and procedures regarding the management of ML/TF/PF risks;
- A clearly articulated ML/TF/PF risk appetite;
- Effective board oversight; and
- A well-defined three lines of defence model.

2

Compliance Officer and Staffing- The board must appoint a Money Laundering Reporting Officer (MLRO) and/or Compliance Officer with the necessary experience and skillset to oversee the LFI's day-to-day AML/CFT/CPF compliance programme. The LFI should ensure the following:

- The Compliance Officer has sufficient authority and resources (monetary, physical, and personnel) to effectively execute their duties;
- The Compliance Officer is sufficiently knowledgeable of applicable AML/CFT/CPF legislation, regulations, guidelines, best practices and must have a comprehensive understanding of the financial institution's risk profile, based on products, services, customers, and geography;
- The development and implementation of a risk-based AML/CFT/CPF Compliance Program;
- That the Compliance function is adequately staffed;
- That there are established clear reporting lines to allow the Compliance Officer to provide timely updates to the board and Senior Management; and
- That there is a documented succession plan, to ensure continuity.

3 **Internal Controls-** An internal control system must be in place at each LFI. Internal controls are the policies and systems which exists within the entity, designed to mitigate and manage ML/TF/PF risks. The system must be applied on a risk-sensitive basis and should be commensurate with the LFI's size, nature and complexity, based on the results of its institutional ML/TF/PF risk assessment. The internal controls system must be documented and approved by the board. The implemented internal controls should be able to achieve the following:

- Identify high risk banking operations;
- Adequately identify and report AML/CFT/CPF compliance deficiencies and monitor the progress of remedial actions taken by management;
- Ensure compliance with legislative requirements;
- Provide sufficient flexibility to allow for regulatory changes or updates to the LFI's risk profile;
- Provide sufficient controls and monitoring systems for timely detection and reporting of unusual and suspicious activity; and
- Ensure that adequate controls and/or segregation of duties for employees directly involved in the identification, monitoring and reporting of ML/TF/PF risks.

4 **Training-** All LFIs must have an implemented AML/CTF/CPF training program. The training program must be adequate and should consider the following:

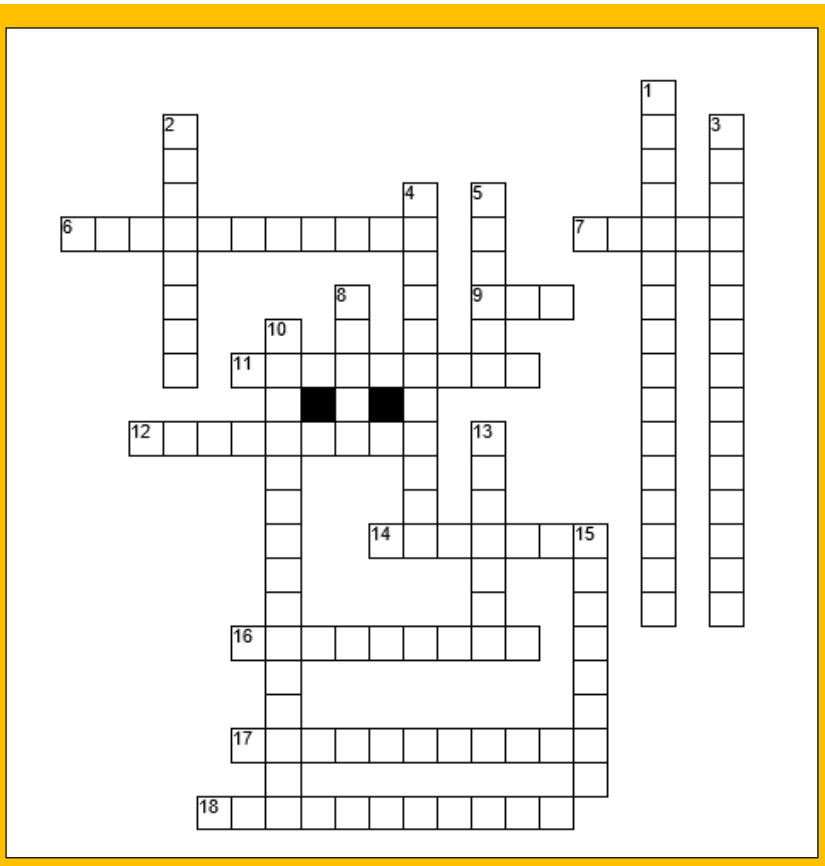
- Training for all employees directly involved with the identification, reporting, monitoring and management of ML/TF/PF risks;
- The training program should be influenced by a needs/gap assessment;
- The training must be tailored to the role and function of the employee and should be periodic;
- Board and senior management must receive specific training to keep abreast of changing trends in ML/TF/PF;
- The frequency of the AML/CFT/CPF training program should at a minimum be aligned to regulatory requirements; and
- Training attendance and materials must be appropriately documented. There must be procedures to ensure that absent employees receive the necessary remedial training.

5 **Independent Assessment-** LFIs must conduct independent testing to assess the adequacy and effectiveness of its AML/CFT/CPF risk management framework. The frequency of independent reviews will be determined by the risk profile of the LFI, based on its ML/TF/PF self-assessment. Independent audits can be conducted by the Internal Audit Department or by a suitably qualified external party. The adequacy of the independent assessment is determined by the following:

- The review should be comprehensive and include an assessment of internal controls, training, staffing and the LFI's compliance with applicable AML/CFT/CPF legislation and internal policies and procedures;
- The information systems should be assessed, including transaction monitoring tools, the applied rules, parameters and the robustness of the system for monitoring and detecting ML/TF/PF risks;
- Sufficient sampling of transactions must be conducted, based on the LFI's size, complexity and ML/TF/PF risk profile; and
- Management responsiveness to addressing deficiencies identified from the independent testing.

A strong governance program is vital to the success of the AML/CFT/CPF program and as such, board and senior management should ensure a strong culture of compliance throughout the institution.

AML CROSSWORD



See page 13 for the answers

Across

6. Stage of ML that would involve purchasing a home
7. Proceeds of _____
9. ___-flags
11. _____ financing
12. Loan repayment & direct deposit are examples of what stage?
14. _____ transaction report
16. The physical entry of illicit funds into the financial system
17. There are generally 3 stages of money laundering: placement, layering, and (_____))
18. transaction designed to evade triggering a reporting or recordkeeping requirement is called

Down

1. component of a more serious crime
2. Involves separating the illicit funds from their criminal source by creating complex layers of legitimate transactions designated to disguise the audit trail
3. disguising illegally obtained funds
4. Integrating the illicit funds into the economy so that they appear to have been derived from a legitimate source
5. can be used to help place proceeds of crime into the financial system and assist with laundering activities
8. _____lines of defence
10. The person or entity that owns or controls 25% or more of the shares of a legal entity
13. Tax (_____) is a predicate offence for money laundering
15. separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds

SECURITY AWARENESS

How can I improve my cybersecurity?

What are cybersecurity risks?

Cybersecurity risk is the probability of exposure or potential loss resulting from a cyber-attack or data breach on your devices or systems.

At the personal and organisational levels, we are becoming more vulnerable to cyber threats due to our increasing reliance on computers and electronic devices, networks and social media.

There are several risks associated with poor cybersecurity, some more serious than others. These may include, an intruder breaking into your system and altering files, malware erasing your entire system, an attacker using your computer to attack others, and a hacker using and stealing your banking details to make unauthorised purchases. The probability of exposure or potential loss resulting from a cyber-attack or data breach on your devices or systems is highest, with the following types of cybersecurity risks:

1. **Malware:** Any unwanted software installed to cause unusual behaviour, which can range from denying access to programs and data using methods like ransomware, deleting files, stealing information, and spreading itself to other systems.
2. **Credential Theft**: Passwords are often the keys to your kingdom and thus a favourite target for compromise.
3. **Social Engineering:** The umbrella method for attempting to deceive users into giving away sensitive details. This includes the frequently used phishing attacks where you may receive an email message appears official, using legitimate appearing information, addresses and requests. Malicious actors have come to realise that it is easier to hack a human and computer.
4. **Traffic Interception:** Techniques used to steal information in which data sent between a user and host is intercepted by a third-party, to listen or eavesdrop on the information.

How can I improve my cybersecurity?

The ubiquity of technology is such that everyone may be exposed to attacks and there are no guarantees even when the best precautionary measures are adopted. However, there are steps that can be taken to minimise the probability of becoming a victim:

1. Identify what are your crown jewels and know where they are stored. Knowing what is most important and valuable to you helps in the decisions about what and how to protect it.

2. Familiarise yourself with the following terms to better understand the risks:
   a. *Vulnerabilities:* these refer to flaws in firmware, hardware, or software that can be exploited by an attacker to gain unauthorised access to your system. Vulnerabilities should be a key focus area in enhancing cybersecurity posture.

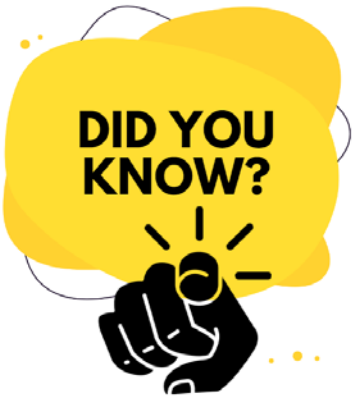
b. Threats: these are malicious acts that seek to access, damage data, steal data, or disrupt digital life in general. Cyber threats can come from within a trusted circle, including family, friends and co-workers or from external by unknown parties.

c. Hackers, intruders, or attackers: these refer to persons who are seeking to exploit weaknesses in computer systems and software for their own personal gain. Sometimes their actions may be benign and motivated by curiosity. However, their actions represent a violation of ethical practices or the intended use of the system they are exploiting.

d. Malicious code: also refer to as malware are unwanted programs or files that may compromise data stored on a computer or cause damage to the device. There are various classifications of malicious codes, these include; trojan horses, viruses, and worms.

3. A proactive approach is the best defence. Seek to understand the threats to your systems and your vulnerabilities, and implement controls to help manage the risk. The following are some basic recommended best practices:

- Always run up-to-date operating system and anti-virus software.
- Use strong passwords: select passwords which will be difficult for attackers to guess. Use unique passwords for different devices and programs. Passwords can be made complex with length (at least 16 characters), the combinations of uppercase and lowercase letters, special characters and numbers. Passphrases usually can be as strong as complex passwords but are easier to remember. Also, the use of a password manager is recommended.
- Change the default usernames and passwords: default usernames and passwords are readily available to malicious actors.
- Implement multi-factor authentication (MFA): the process used to validate a user's identity is known as authentication. MFA uses at least two identity components for authentication, this, therefore, reduces the risk of an actor gaining access to a system in the event your username and passwords are known by the hacker.
- Handle all emails as potentially malicious. Phishing emails are the most common or popular tools used by malicious actors.
- Install firewalls.
- Disable services and connections that are not required.
- Maintain current backups and replications of data to keep ransomware attacks from becoming catastrophic.
- Encryption is usually an effective preventative tool both at the device level and in communication.



MONEY LAUNDERING TYPOLOGY

CASE OVERVIEW

OFFENCE	Money Laundering
CUSTOMER	Individual
INDUSTRIES	Insurance
	Account and deposit-taking institutions (banks)
CHANNELS	Electronic
	Physical transactions
FINANCIAL SERVICES EXPLOITED	ATM Deposit (cash/cheques)
	Third-Party Transactions
	Domestic Wires
SUSPICIOUS ACTIVITY INDICATORS	High value assets acquired with untraceable funds
	Transactions conducted are not consistent with the income level
	Transactions not consistent with subject's profile
	Multiple cash deposits to specific accounts via ATM
	Multiple transfers between personal accounts without apparent cause
	Minimum withdrawal activity despite large balances
	Frequent cash/cheque deposits by/ or in favour of a third-party

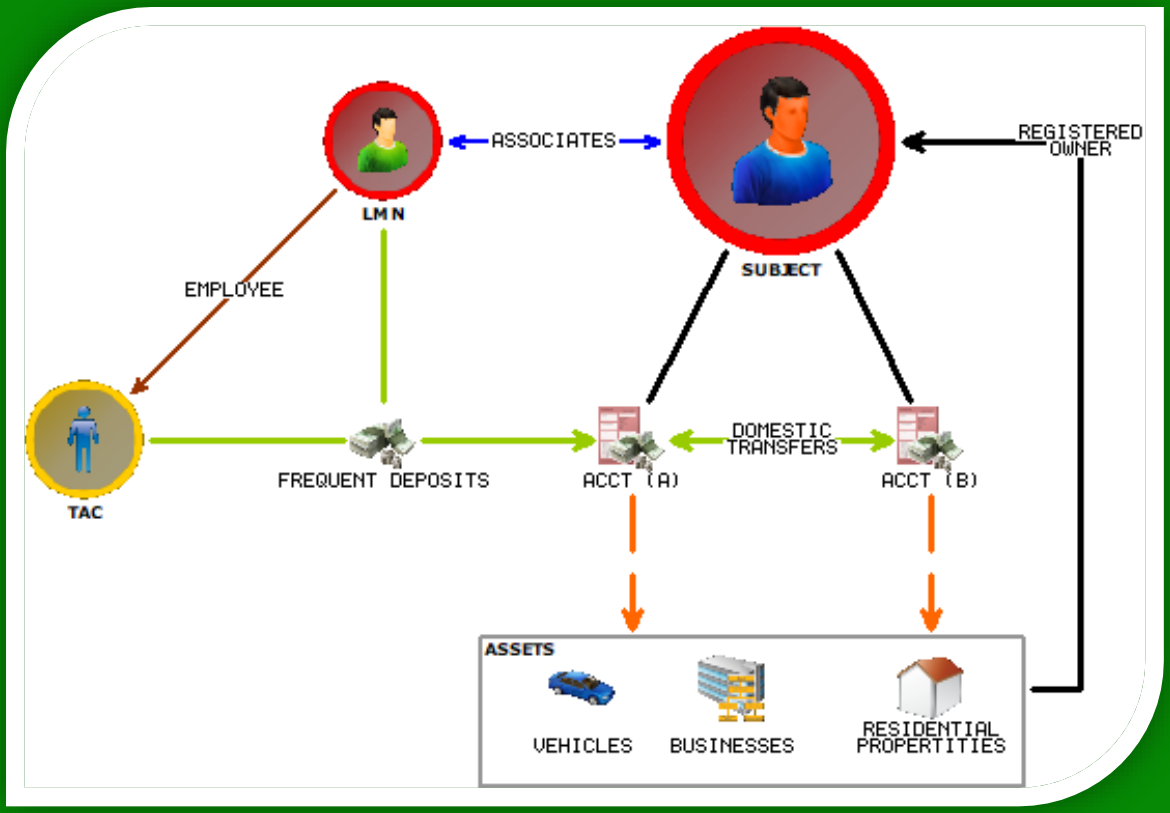
CASE DETAILS

A subject was observed acquiring several high value vehicles within a short period. The vehicles were registered with no security interest and only third-party insurance. Analysis of the individual's income confirmed that declared earnings could not support such purchases. With a rapidly growing asset profile, this prompted the financial activities of the subject to be monitored. Information gathered indicated that funds were frequently being received from a known associate, herein referred to as LMN.

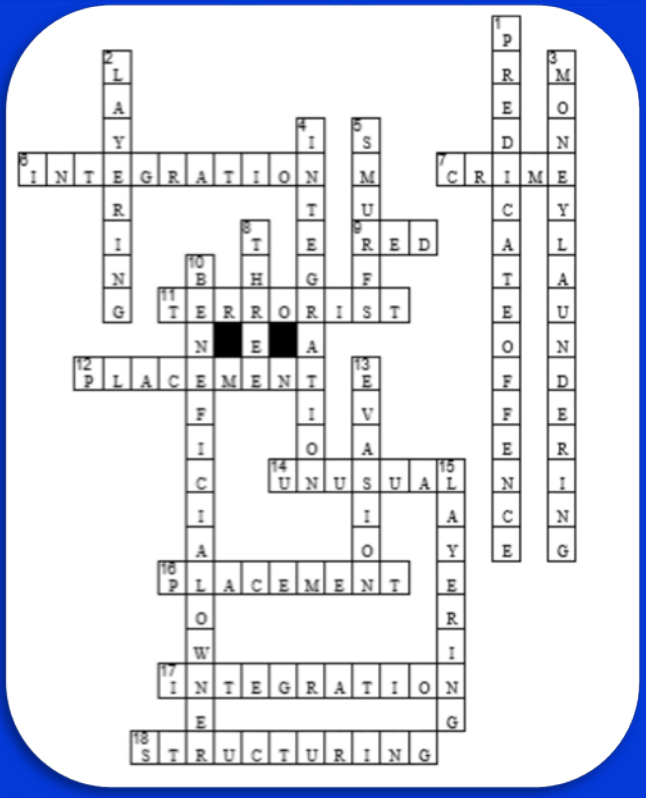
Further analysis revealed the following financial patterns:

- Funds used to purchase assets could not be traced to the accounts of the subject.
- Subject deposited funds significantly in excess of expected activity within a short period of account opening.
- LMN frequently conducted several third-party transactions: ATM or in bank cash/cheque deposits and domestic transfers to the subject's account. LMN maintained accounts with the same institution.
- An employee of LMN conducted multiple cash deposits to the subject's account via the ATM.
- Accounts of the subject primarily funded by LMN, maintained large balances not supported by any declared business activity.
- Frequent transfers of funds between accounts held by the subject at the same institution.
- Very minimal withdrawal activity on accounts associated with LMN.
- The aforementioned transactions conducted by the subject were suggestive of a complex money laundering scheme involving unexplained wealth, the concealment of beneficial ownership, and controlling interest of bank accounts and other assets.

CASE GRAPHIC



Prepared by the Financial Analysis Unit
Office of National Drug and Money Laundering Control Policy – Antigua and Barbuda



Answer Key for puzzle found on page 8.

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/documents

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