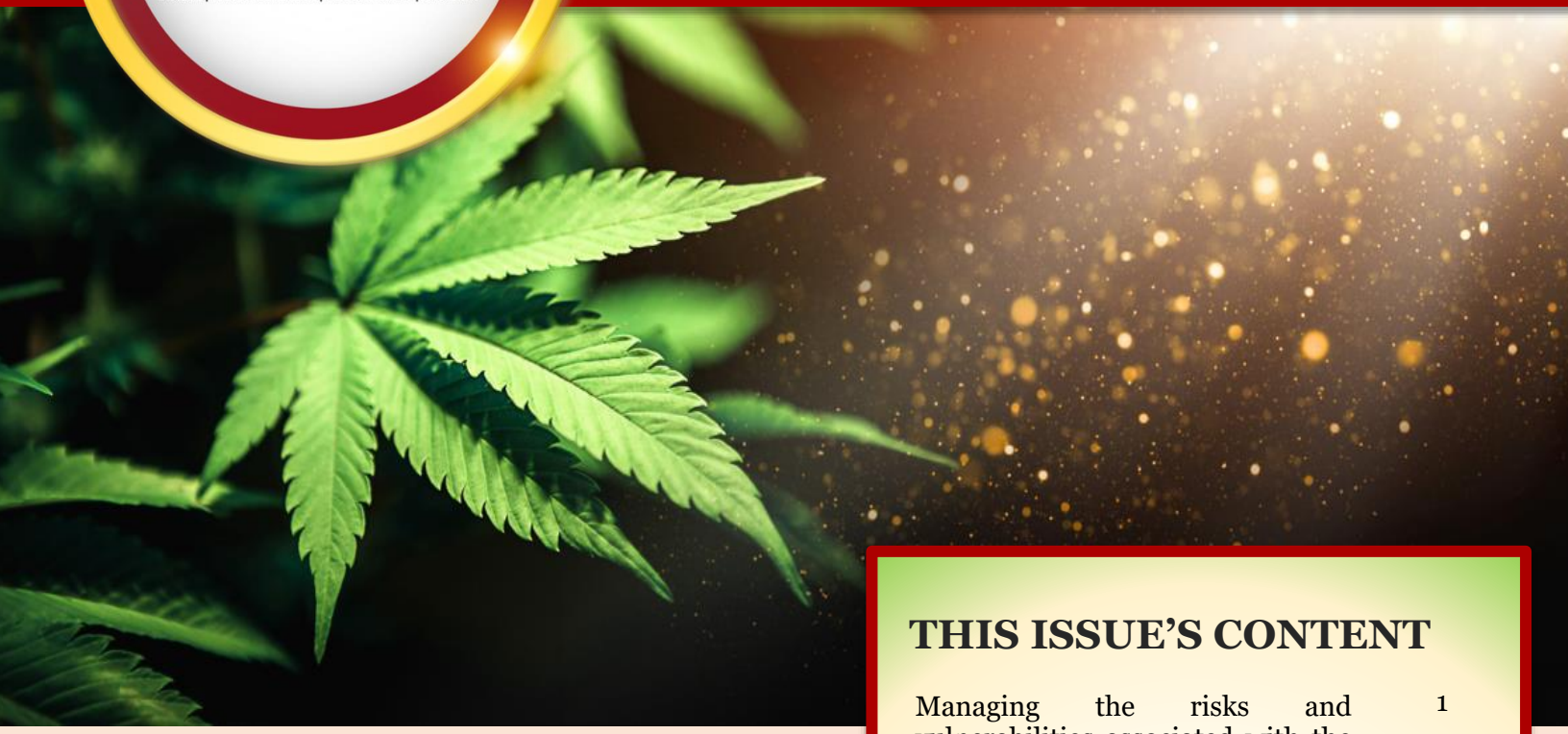
AML/CFT/CPF NEWSLETTER

ISSUE 11 SEPTEMBER



MANAGING THE RISKS AND VULNERABILITIES ASSOCIATED WITH THE MEDICINAL CANNABIS INDUSTRY

In its 2020 flagship report entitled - The Medicinal Cannabis (R)evolution - Challenges in Banking a Burgeoning Industry in the ECCU, the Eastern Caribbean Central Bank (ECCB) noted that the legal use of medicinal cannabis had expanded over the last ten (10) years, as more than thirty (30) countries had legalised the use of the drug for medicinal and therapeutic purposes.

Given the favourable climate and rich agricultural experience in many of the Eastern Caribbean Currency Union (ECCU) member states, the region was viewed as being well-suited to developing a medicinal cannabis industry through a viable domestic and export market. Crucial to this is the facilitation of banking services to facilitate domestic, regional and international transactions.

THIS ISSUE'S CONTENT

Accordingly, the report highlighted the potential predicament faced by licensed financial institutions (LFIs) of preserving correspondent banking relationships, amidst growing concerns regarding money laundering (ML) risk and exploring opportunities that the medicinal cannabis industry may bring to the economies of the ECCU member states.

Medicinal cannabis businesses (MCBs) include those that are engaged in the cultivation, supply, possession and use of products and services related to medicinal cannabis.

LFIs may offer services associated with medicinal cannabis, the decision, however, to offer such services will depend on the risk appetite of the LFI, its business objectives, and its capacity to manage associated risks effectively.

- **MONEY LAUNDERING RISK ASSOCIATED WITH MCBs WITHIN THE FINANCIAL SECTOR**

With the increasing legalisation of cannabis around the world, the industry has flourished, gaining legitimacy and attracting substantial investments. However, the financial sector faces inherent ML risks based on the following:

1. **Cash-intensive nature of MCBs** - MCBs often transact predominantly in cash due to challenges encountered in accessing banking services. This reliance on cash transactions exposes the industry and those who work within to substantial ML risks. While the legalisation of cannabis continues to increase globally, the substance remains illegal in some territories.

2. **Co-mingling of funds** - An influx of untraceable cash presents opportunities for money launderers to invest illicit funds in legitimate cannabis businesses. Laundered money can enter the system as an investment, concealed as legitimate income, and be integrated into the legal financial stream.

3. **Layering and placement techniques** - The cash-heavy nature of the cannabis industry allows for the implementation of sophisticated ML techniques. Criminal entities can exploit the lack of weak compliance systems of LFIs, to obscure the origin of funds through a series of layered transactions, making it difficult to trace the illicit proceeds.

4. **Illegal transfer of funds** - The issue of ML is further exacerbated when attempts are made to transfer funds derived from MCBs across borders to jurisdictions where medicinal cannabis is illegal. This may result in fines, reputational damage, or even criminal liability for both the businesses and the financial institutions involved.

5. **Trade-Based ML** - MCBs are also at risk for trade-based ML schemes. Criminal organisations may use these establishments as intermediaries, disguising their illegal activities through the mixing of legitimate and illegitimate transactions.

6. **De-risking and the loss of correspondent banking relationships** - The ECCB in its report on - The Medicinal Cannabis (R)evolution - Challenges in Banking a Burgeoning Industry in the ECCU outlined the concern that the perceived risk associated with the medicinal cannabis industry, given the historical association of marijuana with illicit drugs, could lead to further severing of correspondent banking relationships in the ECCU; a phenomenon known as de-risking. The concept of de-risking does not only present an issue at the international level, but may also present challenges at the domestic level. On an international level, the perceived ML risks posed by MCBs have resulted in correspondent banks adopting a low risk tolerance for the establishment of relationships with respondent banks that bank the proceeds of MCBs. Accordingly, in an attempt to maintain correspondent banking relationships and lower the risk profile of their institution, some LFIs may also adopt a similar low risk tolerance for banking cannabis proceeds.

- **MEASURES FOR MANAGING THE ML RISKS AND VULNERABILITIES ASSOCIATED WITH MCBs**

As the medicinal cannabis industry advances, it is crucial to address the potential ML risks and vulnerabilities associated with this sector. Robust AML/CFT programmes play a fundamental role in ensuring transparency, accountability, and preventing criminal activities. The following are some key regulatory recommendations to combat ML risks and vulnerabilities associated with providing medicinal cannabis services:

1. **Implementation of a comprehensive AML/CFT/CPF compliance programme:** Developing and implementing a comprehensive anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT/CPF) compliance programme is essential to mitigate ML/TF/PF risks in the medicinal cannabis industry. The programme should include an institutional ML/TF/PF risk assessment that assesses the risks posed by the medicinal cannabis industry, and AML/CFT/CPF policies and procedures that cater specifically to the unique aspects of the industry.

2. **Robust onboarding framework and application of Customer Due Diligence (CDD) measures:** LFIs are required to implement robust onboarding processes for individuals and entities involved in the medicinal cannabis industry. The measures undertaken should be sufficient to mitigate risk and provide management with a reasonable level of assurance that the risk is acceptable, or in keeping with the LFI's ML/TF/PF risk appetite. CDD measures include:

a. Conducting background checks on customers, company directors, shareholders, ultimate beneficial owners, and any associated third parties;
b. Understanding and obtaining information on the purpose and intended nature of the business relationship and verifying the source of funds and source of wealth of customers;
c. Verifying whether the MCB is duly licensed and/or registered in accordance with the relevant national legislation;
d. Collection of due diligence documents from employees within the medicinal cannabis industry such as identification, proof of address, and evidence of employment within the sector;
e. Collection of due diligence documents from entities such as certificates and articles of incorporation, share registers, business plans, financial statements, annual returns, proof of address, and place of business or operations;
f. Requesting from national licensing and enforcement authorities, available information about MCBs and related parties; and
g. Developing an understanding of the normal activity for the business including the types of products to be sold and the type of customers to be served.

The extent to which an LFI will seek additional information beyond those mentioned above will depend on its assessment of the level of risk posed by the customer. Additional information may include, inter alia:

a. Crop inspection or testing reports;
b. Site visits to places of operation or production;
c. Licence renewals; and
d. Updated attestations from MCBs.

3. **Ring-fencing of funds:** LFIs must institute appropriate screening measures to ensure that funds derived from MCBs are not channeled through correspondent banks where medicinal cannabis has not been legalised. Accordingly, LFIs implement mechanisms to ensure that funds associated with MCBs are ring-fenced. Ring-fencing may assist in mitigating de-risking concerns, by ensuring that there are robust monitoring systems such that funds associated with this type of service, is appropriately identified and channeled through the appropriate accounts.

4. **Ongoing monitoring of transactions:** LFIs must conduct ongoing monitoring to identify and report unusual and suspicious transactions related to the medicinal cannabis industry. Periodic reviews and updates should also be conducted on MCBs and employees within the sector, in accordance with their established ML/TF/PF risk profile.

5. **Training and Sensitisation:** Adequate training must be provided to management and staff to enhance their understanding of detecting and preventing of ML/TF/PF activities associated with MCBs. Accordingly, LFIs should communicate employees' obligations in processing related transactions and reporting obligations, where applicable.

6. **Detection and reporting of suspicious transactions:** LFIs should have clear protocols and reporting mechanisms for suspicious transactions, which require reporting to the relevant authorities. Maintaining a robust internal reporting system encourages employees to be vigilant and report any transactions that appear unusual, inconsistent, or suspicious. LFIs should implement risk indicators/triggers to assist in detecting and reporting unusual/suspicious transactions. Such suspicious activity could include the following:
    a. A customer who appears to be engaged in cannabis production in a country or jurisdiction in which cannabis production remains illegal.
    b. A customer appears to be using a MCB as a front, or pretext to launder money derived from criminal activities, or derived from cannabis-related activity that may not be legal.
    c. A customer engaged in cannabis production seeks to conceal or disguise involvement in cannabis-related business activity.
    d. The customer is unable or unwilling to certify or provide sufficient information to demonstrate that it is duly licensed and operating consistent with applicable laws, or the LFI becomes aware that the customer continues to operate (i) after licence revocation, or (ii) inconsistently with applicable laws.
    e. A MCB receives substantially more revenue than may be reasonably expected or than its local competitors.
    f. A MCB is depositing more cash than is commensurate with the amount of business revenue reported in its financial statements.
    g. A MCB is unable to demonstrate that its revenue is derived exclusively from the provision of medicinal cannabis-related services.
    h. Deposits made by a MCB appear to be structured, to avoid currency transaction report requirements.
    i. Deposits by third parties with no apparent connection to the account holder.
    j. Excessive commingling of funds with the personal account of the MCB owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
    k. Individuals conducting transactions for a MCB appear to be acting on behalf of other, undisclosed parties of interest.
    l. Financial statements provided by a MCB are inconsistent with actual account activity.
    m. A surge in activity by third parties offering goods or services to MCBs such as equipment suppliers or shipping services.

7. **Independent reviews:** An effective third line of defense should be established for assessing the adequacy of established controls to manage and mitigate the risks posed by the medicinal cannabis industry. Independent auditors should have a thorough understanding of the expected activity in the medicinal cannabis industry, the associated governing laws, what types of reviews and processes are carried out by the LFI and what types of risks are present within the banking sector. Audits conducted may include an assessment of procedures for onboarding customers, the established CDD framework, and the risk management guidelines to assess the effectiveness of policies and internal controls.

8. **Cooperation:** Given the global nature of the medicinal cannabis industry, national, regional and international cooperation is paramount in addressing ML/TF/PF risks. Collaborative efforts between regulators, institutions and jurisdictions can help in the sharing of intelligence, exchanging information, and enhancing the overall effectiveness of AML/CFT/CPF initiatives.

By implementing the above measures, LFIs can effectively mitigate the ML risks and vulnerabilities associated with the rapidly growing medicinal cannabis industry. It is important to continually update and adapt these measures as the industry evolves, ensuring that compliance remains one step ahead of potential illicit activities.

On 22 July 2016, the Monetary Council, at its 85th meeting, took the decision to recommend to member governments that the legal responsibility for AML/CFT supervision and regulation of financial institutions licensed under the Banking Act, 2015 be transferred to the ECCB.

The recommendation to designate the ECCB as the regulatory authority for AML/CFT for its licensees was necessary to address deficiencies relating to AML/CFT supervision that were cited in the Caribbean Financial Action Task Force (CFATF) Mutual Evaluation Reports. Additionally, there was need to promote uniformity and consistency regarding the application of an AML/CFT supervisory framework to address some of these deficiencies.

THE ROLE OF THE ECCB AS AML/CFT SUPERVISORY AUTHORITY

In 2018, the ECCB implemented its Risk Based Supervision Framework for prudential supervision of its licencees. The Risk Based Supervision Framework describes the principles, concepts and core process which the ECCB utilises to supervise LFIs. In this regard the ECCB has strategised its mission to balance prudential supervision with AML/CFT/CPF supervision to ensure an integrated approach to supervision.

The ECCB is the named AML/CFT/CPF Supervisory Authority for LFIs in Antigua and Barbuda, the Commonwealth of Dominica, Grenada, Saint Lucia and Saint Vincent and the Grenadines, as such all LFIs under the Banking Act, 2015 in the named jurisdictions are subject to the ECCB's AML/CFT/CPF Risk Based framework.

The role of the ECCB as an AML/CFT/CPF Supervisor is multi-faceted, and includes the following:

1. **Implementing effective market entry controls** – Fitness and probity assessments are meant to prevent criminals or their associates from owning, controlling, holding a significant or controlling interest, or a management function in a LFI. Such controls are applied at the time of initial licensing or registration of the LFI, and on an ongoing basis. Fit and proper assessments are conducted on beneficial owners, directors, members of senior management, and officers of LFIs. Where applicable, the AML/CFT Compliance Officers and ML Reporting Officer must be approved by the ECCB upon completion of a successful fit and proper assessment.

2. **Understanding and assessing ML/TF/PF Risk -** The ECCB maintains an understanding of the ML/TF/PF risks within the banking sector and in individual LFIs through its off-site and on-site supervisory activities, as well as information provided in the respective ECCB member countries ML/TF National Risk Assessments (NRA). The ECCB utilises a risk matrix to prioritise institutions for inspections, based on the assigned ML/TF/PF risk profile. The ongoing assessment and understanding of risks provides a basis for the development and application of the ECCB's AML/CFT/CPF risk based supervisory programme and strategies.

3. **Supervise and monitor LFIs to ensure their effective assessment and management of ML/TF/PF risk and compliance with AML/CFT/CPF preventive measures through:**
    a. The conduct of risk based AML/CFT/CPF off-site and on-site inspections; and
    b. The issuance of remedial actions to correct weaknesses in LFIs AML/CFT/CPF processes, procedures, systems or controls, and to influence and foster a compliance culture that contributes to effective risk management.

4. **Enforcement of Remedial Actions and Sanctions** - As AML/CFT Supervisory Authority, the ECCB must be able to demonstrate that its actions have an effect on compliance by LFIs. Accordingly, in keeping with the requirements of the Financial Action Task Force (FATF) Recommendation 35, the ECCB applies a range of remedial actions and sanctions as outlined in its Ladder of Enforcement document. This assists with addressing identified weaknesses in LFIs risk management systems, mitigate ML/TF/PF risks in a timely manner and ensures compliance with AML/CFT/CPF obligations. These include Letters of Commitments, Memoranda of Understanding, Directives, Administrative Penalties and Revocation of Licences**.**

5. **Guidance and Feedback** – These are provided to LFIs to ensure that clear, relevant, meaningful and up-to-date, AML/CFT/CPF related information is made available on an ongoing basis. These can be communicated in various ways, and may include changes to the AML/CFT/CPF regulatory framework, issuance of supervisory letters and examination reports, explanation of the AML/CFT/CPF regulatory requirements, provision of relevant typologies, updates and training on ML/TF/PF vulnerabilities, risks and threats, and regulatory expectations. The ECCB is also mandated to develop and issue standards and guidelines in relation to AML/CFT/CPF.

6. **Supervisory Coordination and Cooperation** – A Multilateral Memorandum of Understanding (MMOU) was established in 2018 between the ECCB and relevant AML/CFT authorities in ECCU member countries, for collaboration on matters relating to AML/CFT. The scope of the MMOU is to promote the mutual assistance and exchange of information amongst the competent authorities to enable the authorities to perform their respective duties and functions effectively according to law. Accordingly, coordination and cooperation occurs in drafting amendments to national AML/CFT/CPF legislation, conducting ML/TF NRAs, conducting AML/CFT/CPF training, joint inspections and sharing of relevant information.

REGULATORY UPDATES

THE LAUNCH OF THE ECCB VIRTUAL AML/CFT/CPF LEARNING CAMPUS

1

In February 2022, the ECCB introduced its Association of Certified Anti-Money Laundering Specialists (ACAMS) Enterprise Membership Programme which provides members with a learning platform to facilitate ongoing capacity building as it relates to AML/CFT/CPF matters. On 12 September 2023, the ECCB launched a new approach to the administration of the enterprise membership with the launch of its AML/CFT/CPF Virtual Campus. The ECCB will identify a number of webinars which participants are required to complete on a quarterly basis. This is to ensure that topical areas based on identified deficiencies and new and emerging ML/TF/PF risks are being covered by enterprise members, and to ensure that members maximise the benefits offered by the programme. The enterprise members consist of individuals from various regulatory bodies and compliance personnel from LFIs within the ECCU.

SAINT LUCIA ANNOUNCES THE COMPLETION OF ITS 2022 ML/TF NATIONAL RISK ASSESSMENT

2

In September 2023, Saint Lucia announced the completion of its 2022 ML/TF NRA. The NRA, which covered the period 2018-2022, was led by the National Anti-Money Laundering Oversight Committee, with participation from the various competent authorities in Saint Lucia, as well as members from the private sector. The NRA is critical to Saint Lucia's application of its risk-based approach to AML/CFT, as well as ensures compliance with the FATF Recommendation 1. This is the second time in which Saint Lucia has conducted a NRA, having completed the first NRA in 2019. The country has taken a proactive approach towards the identification of ML/TF risks, given the dynamic risk environment that it continues to operate within. The overall ML risk to Saint Lucia was assessed as **medium** while the overall TF risk was assessed as **medium-low**. The domestic banking sector overall ML risk was assessed as **medium**.

THE CFATF PUBLISHES THE 4TH ROUND MUTUAL EVALUATION REPORT OF THE COMMONWEALTH OF DOMINICA

3

The Caribbean Financial Action Task Force (CFATF) published the 4th round Mutual Evaluation Report (MER) of the Commonwealth of Dominica ('Dominica') in July 2023. The MER, which was adopted at the CFATF Plenary held in Trinidad and Tobago in May 2023, summarises the AML/CFT measures in place in Dominica as of the date of the on-site visit, which was conducted over the period 15 to 26 August 2022. Additionally, the report analyses the level of compliance with the FATF 40 Recommendations, the level of effectiveness of Dominica's AML/CFT system and provides recommendations on how the system could be strengthened.

https://www.cfatf-gafic.org/home/cfatf-news/799-the-4th-round-mutual-evaluation-of-the-commonwealth-of-dominica

OFAC PUBLISHES LATEST EDITION OF SDN AND BLOCKED PERSONS LIST

4

The Office of Foreign Assets Control (OFAC) of the United States Treasury Department issued an updated list of Specially Designated Nationals (SDN) and Blocked Persons on 19 September 2023. The SDN list contained organisations and individuals who were restricted from doing business with the United States, American companies or Americans. It includes terrorist organisations, individual terrorists, state sponsors of terrorism and traffickers in narcotics and weapons of mass destruction. Prior to this, the OFAC issued notices of updates to the SDN and Blocked Persons List on 31 July 2023 and 12 September 2023.

https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

THE EU ESTABLISHES AUTONOMOUS HAITI SANCTIONS FRAMEWORK

5

On 28 July 2023, the European Union (EU) Council announced amendments to its sanctions regime to allow for the autonomous imposition of restrictive measures against individuals and entities responsible for threatening the peace, security or stability of Haiti. The EU initially imposed sanctions on Haiti in October 2022, in line with those established by the UN Security Council. The updated amendments allow the EU to autonomously impose a travel ban for individuals and the freezing of funds belonging to both individuals and entities. The EU noted that the updated amendments were made in light of high levels of gang violence and other criminal activities, sexual and gender-based violence, embezzlement of public funds, ongoing impunity for perpetrators, as well as the dire humanitarian situation in Haiti.

https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/haiti-eu-sets-up-autonomous-framework-for-restrictive-measures/

AML/CFT MENTORSHIP EXTENDED IN MONTSERRAT

Montserrat is the sixth ECCU country to have benefited from the ECCB's AML/CFT Mentorship Programme. This was made possible through the Caribbean Development Bank's 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.

The ECCB, through the provision of technical support, assisted the Financial Services Commission (FSC) in Montserrat in the conduct of a risk based AML/CFT/CPF examination. As a part of the preparations for the execution of the examination, the ECCB facilitated AML/CFT governance training for the FSC. The ECCB also met with Governor Sarah Tucker to discuss Montserrat's progress with refining its systems in the global fight against ML/TF/PF and the implementation of its a risk-based supervision framework.

To date, the Commonwealth of Dominica, Grenada, Saint Christopher (St Kitts) and Nevis, Saint Lucia, and Saint Vincent and the Grenadines, have also benefited from the mentorship programme.

Photographed: Representatives of the ECCB, Governor's Office - Montserrat, Financial Services Commission- Montserrat, Financial Crime and Analysis Unit – Montserrat

By the Management Information Systems Department - ECCB

October 2023 is Cyber Security Awareness month and the theme for this year is "*It's easy to stay safe online*." The latest data shows over 5.18 billion active internet users globally, representing approximately 64.6 per cent of the global population. With the high levels of phishing and other cyber-attacks, more individuals and organisations have experienced at least one type of cyber-attack related to online activities. It is therefore opportune to highlight the ongoing threats that individuals and organisations face, and the need to ensure cyber security awareness at all levels. **There are simple ways to protect individuals, families and businesses from online threats, and practicing the basics of cybersecurity can make a huge difference.**

The goals for Cyber Security Awareness month 2023 is to make actionable steps positive, approachable, simple and taken back to the basics by focusing on four (4) key behaviours:

- Using strong passwords and a password manager;
- Enabling multifactor authentication;
- Updating software; and
- Recognising and reporting phishing.

Passwords are the keys to the digital kingdom and are similar to home and office keys, as such measures should be taken to keep passwords safe. All passwords should be created with the guiding principles of adequate length, uniqueness and complexity. There are varying schools of thought on how often passwords should be changed. However, any decision should be based on the application of the aforementioned principles, as well as other additional authentication methods that have been implemented, including multifactor authentication (MFA). Passwords should be changed if an unauthorised person has accessed the account, or the password was identified as compromised in a data breach. As password length and complexity can make them difficult to remember, the use of a password manager vault is also highly recommended. As a reminder, the password for the password manager vault should also comply with the same guiding principles.

Multifactor authentication allows for account protection in multiple ways and requires the user logging in to prove their identity including something you know (username, password, pin), something you have (token code, email, phone, app) and something you are (fingerprint, retina, face). MFA is often used in the form of two-factor authentication and this complicates the process of unauthorised access to accounts, even if the password is known. It is therefore highly recommended that MFA be implemented for any account that permits it, especially accounts associated with banking, work, social media, email and online stores.

Despite being one of the best ways to secure account authentication, MFA is not the panacea for account compromises as there have been instances where it has been circumvented by cybercriminals. Users are therefore still required to exercise due diligence in handling MFA log-in requests, unknown MFA requests should not be approved and it's a good reason to change the password for the account.

Updated software on systems and devices is one of the more effective ways to enhance security posture. Malicious actors are constantly searching for vulnerabilities in software and apps, configuring devices to automatically update from authentic vendor sources. Periodically checking software update settings, is a minimum requirement for minimising the risk of compromise.

Notwithstanding, complex passwords reinforced by MFA and updated devices, many cyber-attacks are in fact still hard to detect and even more difficult to stop. Social engineering techniques, particularly phishing and spear phishing is a preferred method of cyber criminals as they help to circumvent controls, relatively easy and are inexpensive to implement. Being equipped with the knowledge and established practices to recognise fraudulent emails, social media posts or direct messages with the objective of enticing recipients to click on a malicious link or download an unwanted attachment is critical.

Romance Scam

CASE STUDIES

Romance scams occur when criminals create fake identities, usually online, with the aim of gaining the victim's trust and convincing them that they are in a genuine relationship, to eventually persuade and exploit these victims for money for variety of emotive reasons. Requests are usually the need for money for business ventures, medical care, and living expenses. According to the December 2022 Global Financial Integrity Report on Financial Fraud in the Caribbean, romance scams were among the most common types of fraud in the Caribbean. Criminals targeted older people and those who may have been struggling in a relationship and/or were emotionally vulnerable. Victims of romance scams suffered both emotional and financially damages.

CASE 1

Scammer - Two women ages 29 and 52, and a 52-year-old man
Victim – Three men, ages 50, 70 and 70

What happened? – The three (3) scammers attracted three (3) victims using a newspaper dating ad, posing as a widowed 50-year-old woman. The victims believed they were paying for a legitimate dating service and provided money to their love interest, to assist with a difficult work situation. After the perpetrator (the supposed widow) stopped replying, one of the men grew suspicious and prompted the police to open an investigation. Another, encouraged by a friend to consider the possibility that he was being scammed, also contacted the authorities.

Loss – The two (2) men who reported the scam lost approximately Australian Dollar (AUD) 42,000 and AUD 343,500, respectively. The third victim lost over AUD 111,000 between June 2022 to February 2023.

READ MORE https://mypolice.qld.gov.au/news/2023/09/07/romance-scam-arrests-gold-coast/

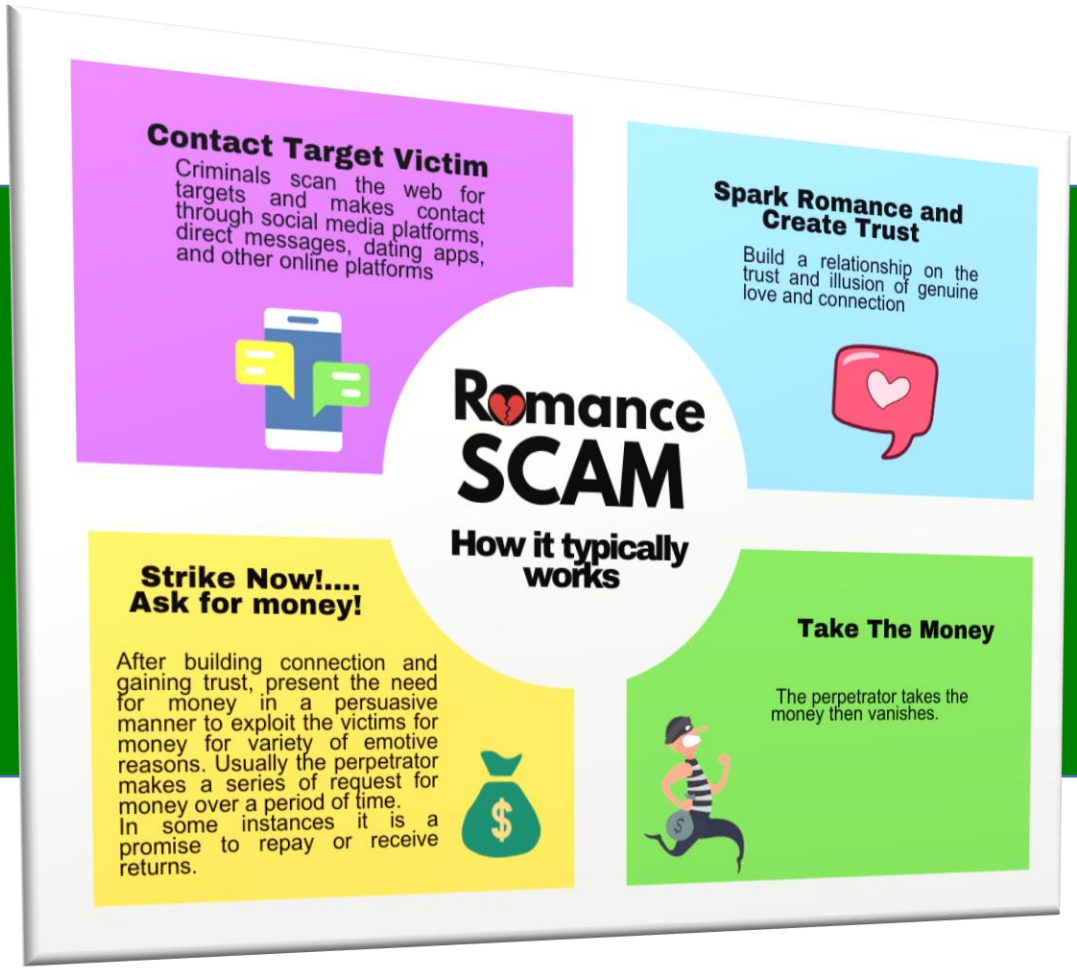
CASE 2

Scammer – 36-year-old woman
Victim – 87-year-old man

What happened? – The two met on a dating website. The scammer convinced the victim that she needed money for an attorney withholding money from an injury settlement and, in a separate request, stated she needed money to gain access to a bank account from which she would repay the victim money.

Loss – The victim wrote sixty-two (62) cheques to the perpetrator totalling over USD2.8m. The victim lost his life savings and his apartment, while the scammer bought herself a home in a gated community, a condominium, a boat, several luxury cars and rolex watches.

READ MORE https://www.justice.gov/usao-sdny/pr/florida-woman-sentenced-51-months-prison-defrauding-holocaust-survivor-28-million



Preventing Romance Scams

- ✓ Research a person's photograph and profile utilising online searches to determine whether the images, name or details have been used elsewhere.
- ✓ Take the relationship slow and ask a lot of questions.
- ✓ Beware of individuals who may appear too perfectly matched.
- ✓ Beware if an individual appears to quickly want to leave a dating app to communicate directly (outside the dating app/website).
- ✓ Beware if an individual keeps promising to meet in person but always has an excuse for not being able to show up.
- ✓ Beware of attempts to isolate you from your friends and family.
- ✓ Beware of the requests for money.
- ✓ Never send money to anyone you have only communicated with online or by phone.

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