AML/CFT NEWSLETTER

ISSUE 8 DECEMBER 2022

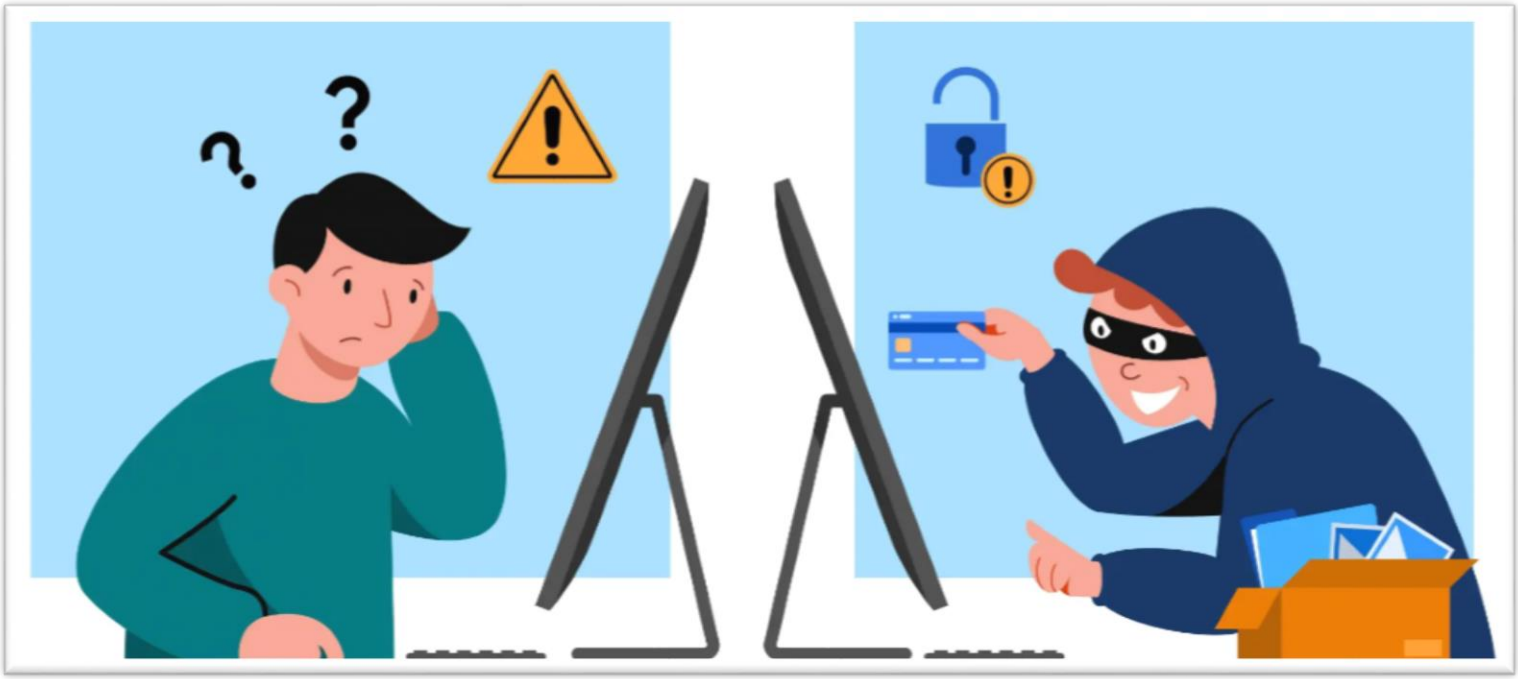
A RISE IN FRAUD. BE ALERT!

Member countries of the International Criminal Police Organization (INTERPOL) have frequently identified money laundering (ML) and financial fraud as representing a 'high' or 'very high' threat. The *2022 INTERPOL Global Crime Trend Summary Report* highlighted as rates of digitalization rapidly accelerated, particularly during the pandemic, it was noted that online social engineering of financial fraud, victim manipulation and impersonation scams increased significantly.

A publication by Global Financial Integrity on *Financial Fraud in the Caribbean*, highlighted an increase in financial crimes in the Caribbean including fraud schemes. Further, the report outlined that financial fraud had a wide footprint across the region, involving hundreds of millions, if not billions of dollars in illicit proceeds each year, which impacted the economic security of countries and the region.

THIS ISSUE'S CONTENT

The Financial Action Task Force (FATF), in its publication - *COVID-19-related Money Laundering and Terrorist Financing, Risks and Policy Responses* reported that its members, observers, and open sources indicated that criminals attempted to profit from the COVID-19 pandemic through increased fraudulent activities.



Source: Payments Journal

Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim.

It occurs "*when a person or business intentionally deceives another with promises of goods, services, or financial benefits that do not exist, were never intended to be provided, or were misrepresented*."[1] Financial fraud, therefore, involves deception involving financial transactions and comprise a variety of scams and schemes. Opportunity represents one of the main drivers of fraud and the increased use of technology has made it easier for criminals to perpetrate fraud on their victims.

The publication, *Financial Fraud in the Caribbean,* reported that the most common fraud types in the Caribbean are advance fee frauds, specifically lottery/prize scams, online shopping scams, and romance scams, as well pyramid and Ponzi schemes. The report further outlined that pyramid schemes in the region frequently took advantage of citizens' comfort and familiarity with "sou-sous", a legitimate, informal community savings practice.

According to United Kingdom (UK) Finance, a trade association for the UK banking and financial services sector, "*social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, continued to be the key driver of both unauthorised and authorised fraud losses in the first half of 2022*".[1] The association highlighted criminals' use of scam phone calls, text messages and emails, as well as fake websites and social media posts, to trick people into handing over personal details and passwords. This information was then used to target victims and convince them to make payments to the criminals.

1 Financial Fraud in the Caribbean, December 2022

The *Financial Fraud in the Caribbean* reported that the channel of communication may be shifted, as the fraud progresses, to enable the fraudster to stay ahead of law enforcement and to ensure that suspicions are not aroused. The report indicated that the primary channels used to move the proceeds of fraud in the Caribbean were cash smuggling, small transactions via money service businesses, bank transfers, trade-based money laundering, and online money transfer platforms.

Licensed Financial Institutions (LFIs) should note that criminal activity, including fraud, generates proceeds that criminals must launder. Therefore, it can be reasonably presumed, where there is fraud, there is ML. It is imperative that LFIs implement the appropriate systems and controls to identify, report, and prevent fraud. Fraudsters continuously and rapidly perpetrate attacks on victims through various channels. To prevent fraud, LFIs should ensure that a risk assessment of its security framework and vulnerability of delivery channels is conducted and that appropriate mitigating controls are instituted.

Six tips to improve LFIs' Security Systems:

1. Be aware of the types of fraud and their various contact channels;
2. Educate customers and employees on fraud and mitigating techniques;
3. Develop and implementing fraud prevention policies and procedures;
4. Implement an ongoing fraud monitoring system;
5. Implement a system of internal controls for the testing and auditing of security systems; and
6. Alert customers when fraudulent or suspicious activities are detected.

Sources

1. **2022 INTERPOL Global Crime Trend Summary Report**: available at file://ctxfile01/CitrixUserData/lj1177.ECCBDOM/Downloads/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf
2. **Financial Fraud in the Caribbean, December 2022**, by Channing Mavrellis: available at https://gfintegrity.org/wp-content/uploads/2022/12/GFI-Financial-Fraud-in-the-Caribbean.pdf
3. **2022 Half Year Fraud Update** by UK Finance in association with Lexis Nexis Risk Solutions: available at https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf
4. **COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses,** by the FATF: available at file://ctxfile01/CitrixUserData/lj1177.ECCBDOM/Downloads/COVID-19-AML-CFT.pdf

REGULATORY UPDATES

FATF: Results of FATF Plenary- Paris (October-November 2022)

The first Plenary of the FATF under the Presidency of T. Raja Kumar of Singapore, took place in Paris on 20-21 October 2022.

The Plenary discussed the ongoing Russian invasion of Ukraine and further restrictions were placed on Russia's FATF membership. Following the statements issued in March, April and June 2022, the FATF reiterated that all jurisdictions should be vigilant to emerging risks from the circumvention of measures taken against Russia in order to protect the international financial system.

FATF members agreed to release draft guidance for public consultation related to Recommendation 24 concerning beneficial ownership transparency for legal persons and proposed amendments to Recommendation 25, which aims to improve beneficial ownership transparency for trusts and similar legal arrangements. The FATF expects to finalise these revisions in February 2023.

The plenary also held discussions centered around:

- Additions to the blacklist;
- Changes to the grey list;
- Improving asset recovery;
- Undertaking new projects to enhance global anti-corruption efforts; and
- Providing guidance on detecting and disrupting illegal fentanyl trafficking.

READ MORE https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-october-2022.htm

Updates to FATF Black and Grey Lists

On 21 October 2022, the FATF added Myanmar to the "black list", citing its failure to make enough progress in fully addressing its AML/CFT deficiencies. Additionally, the FATF noted Pakistan and Nicaragua progress in improving the elements of its AML/CFT regime and as such were removed from the "grey list".

READ MORE https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

European court rules against EU on beneficial ownership

The European Court of Justice (ECJ) on 22 November 2022, decided that open public access to the beneficial owner registers of European Union (EU) member state companies was no longer valid. The court ruled that registers containing the personal details of the owners of a company and accessible to the general public is an infringement of fundamental rights of privacy and personal data protection. Bermuda has long resisted efforts to make beneficial ownership registers public. Former Finance Minister Bob Richards stated that the ruling was good news for Bermuda. This ruling is seen as a decision that could stall global efforts to force countries to have open beneficial registers.

READ MORE https://www.royalgazette.com/international-business/business/article/20221123/european-court-rules-against-the-eu-on-beneficial-ownership/

AML/CFT MENTORSHIP PROGRAM EXTENDED IN GRENADA

Representatives of the Eastern Caribbean Central Bank (ECCB) with members from the AML Commission – Grenada.

The ECCB, through the provision of technical support, continues to assist member countries in the conduct of risk-based examinations. The ECCB's mentorship train headed to Grenada during the period 17 to 28 October 2022. The ECCB conducted practical training session with the AML Commission - Grenada, on the conduct of a risk-based AML/CFT/CPF examination of a financial institution in Grenada. The training covered:

- Pre-onsite preparations;
- Pre-onsite training on conducting the examination and interview preparations;
- Conduct of the examination;
- Drafting the examination report; and
- How to conduct follow up action.

The mentorship program is made possible through the Caribbean Development Bank (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 Eastern Caribbean Currency Union (ECCU) member countries, in keeping with international best practices. The project kicked off in February 2022. To date, the Commonwealth of Dominica, Saint Lucia, Saint Vincent and the Grenadines, and Saint Christopher (Kitts) and Nevis have also benefited from the mentorship program.

SIGNING OF MOU BETWEEN ECCB AND SAINT LUCIA'S FINANCIAL INTELLIGENCE AUTHORITY TO IMPROVE COOPERATION

Mr Paul Thompson, Director, FIA, Saint Lucia is pictured signing the MMOU

In November 2021, The Saint Lucia Money Laundering Prevention Act No. 8 of 2010 (the Act/MLPA 2010) was amended to appoint the Eastern Caribbean Central Bank as the Anti-Money Laundering Supervisory Authority for financial institutions licensed to carry on banking business under the Banking Act Cap.12.01.

In accordance with Section 5 (2) (h) of the MLPA 2010, in November 2022, the Saint Lucia Financial Intelligence Authority (FIA) signed on to a Multilateral Memorandum of Understanding (MMOU) amongst the Eastern Caribbean Central Bank (ECCB) and other national regulators. The MMOU outlines the provisions for cooperation and exchange of information and collaboration between agencies, in order to exercise powers relative to anti-money laundering, counter-terrorist financing and counter-proliferation financing matters.

PRESS RELEASE

SAINT LUCIA
ATTORNEY GENERAL'S CHAMBERS
NATIONAL RISK ASSESSMENT WORKSHOPS

The Attorney General's Chambers recently concluded a National Risk Assessment (NRA) Workshop with stakeholders from the public and private sector. This workshop was held over two (2) days 15-16 November at the Bay Gardens Resort. The workshop saw seventy-two (72) participants who were sensitized about the NRA process and a World Bank Tool by presenters such as Mrs Nathalie Dusauzay, Ms Ayanna Caesar and Ms Kozel Creese. Participants were encouraged to join teams, each examining a specific sector in Saint Lucia inclusive of banking, non-profit organizations, legal persons, designated non-financial businesses and professions and virtual asset and virtual asset service providers. The Attorney General Mr. Leslie Mondesir in his opening remarks, highlighted the national importance of this activity and reinforced the Government's commitment and support in the fight against money laundering, terrorist financing and countering the financing of weapons of mass destruction.

Members of the National Anti-Money Laundering Oversight Committee

The Caribbean Financial Action Task Force (CFATF) is a regional body which conducts evaluations across the Caribbean to determine a country's compliance in combating money laundering, terrorist financing and the proliferation of weapons of mass destruction. Saint Lucia will be undergoing its re rating process following the publication of its fourth round mutual evaluation by the CFATF in 2021. The NRA report is a fundamental requirement and a second workshop with these teams is scheduled for early 2023 to validate the revised NRA. The accuracy of the information provided will assist the Government in allocating limited resources to its most vulnerable areas when addressing Saint Lucia's threats with respect to money laundering and terrorist/counter proliferation financing.

As part of the re- rating process, Saint Lucia will also sign a Memorandum of Understanding with competent authorities such as, the Attorney General's Office, Director of Public Prosecutor's Office, Royal Saint Lucia Police Force, Customs and Excise Department, Inland Revenue Department, Financial Intelligence Authority, Financial Services Regulatory Authority and the Eastern Caribbean Central Bank to enhance issues of coordination and cooperation in sharing of information. Such an initiative will strengthen the existing Anti Money Laundering/Counter Financing Terrorism /Counter Proliferation Financing controls in the island.

Members of the Banking Sector Working Group consulting with representatives of the domestic and international banking sector

Members of the Financial Institutions Working Group

TARGETED FINANCIAL SANCTIONS

Under Chapter VII of the United Nations Charter, The United Nations Security Council (UNSC) can take action to maintain or restore international peace and security. Pursuant to Article 41, sanctions measures encompass a wide range of enforcement options, exclusive of the use of armed force. In pursuit of a variety of goals, UNSC sanctions can assume several forms. The measures can range from comprehensive economic and trade sanctions to more targeted measures such as, arms embargoes, travel bans, and financial or commodity restrictions. Sanctions have been applied to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and counter-proliferation efforts.

Targeted Financial Sanctions (TFS) refer to sanctions imposed by the UNSC against identified individuals, groups, or undertakings for matters relating to ML, terrorist financing (TF), political conflicts, and nuclear proliferation. TFS aims to restrict access to funds, economic resources, or financial assets of any kind to sanctioned persons.

FATF Recommendation 7 requires countries to implement TFS to comply with the UNSC's resolutions. Countries are required to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person or entity designated by the UNSC under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions.

LFIs must ensure that all customers, existing and new are screened against the United Nations sanctions lists: https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

Screening should be comprehensive and include complete customer data. Surface screening of the customer may be inadequate. LFIs should therefore include information such as customers' full names, names of related parties (suppliers/customers), and names of beneficial owners and directors or agents when screening. Where possible, names should be searched in combination with additional parameters such as date of birth or date of incorporation, address, aliases, nationality of individuals, place of incorporation and jurisdiction of operation.

CULMINATION OF ECCB - WORLD BANK RISK BASED ASSESSMENT TOOLKIT TRAINING SERIES

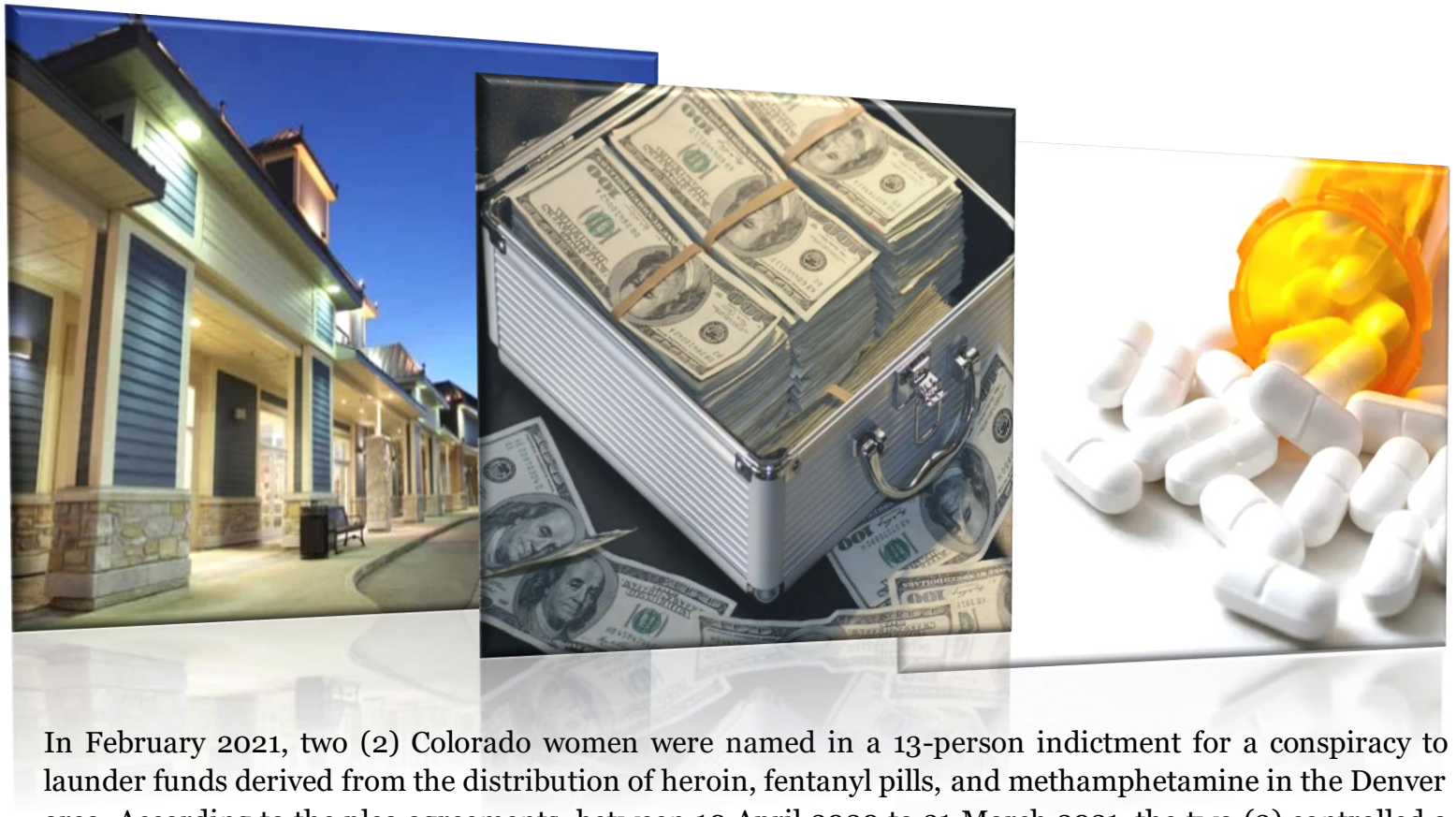
The World Bank Risk-Based Approach (RBS) Toolkit training series, culminated in a closing workshop held in Miami, during the period 12-14 December 2022. The workshop, hosted by the World Bank in collaboration with the ECCB, was attended by regulators and supervisors from the CARIFORM countries of Antigua and Barbuda, Commonwealth of Dominica, Grenada, St Christopher (Kitts) and Nevis, Saint Lucia and Saint Vincent and the Grenadines.

The RBA toolkit training series included a suite of seven (7) interrelated modules and templates, which supported AML/CFT supervisors in developing and enhancing practical skills to create an effective regulatory environment and to implement a RBA.

The World Bank provided technical assistance with funding by the European Union. Module 1 of the training series was held on 15 April 2020 and was attended by national supervisory authorities across the ECCU.

MONEY LAUNDERING CASE STUDY

Structuring through the use of a U.S cash-intensive business



In February 2021, two (2) Colorado women were named in a 13-person indictment for a conspiracy to launder funds derived from the distribution of heroin, fentanyl pills, and methamphetamine in the Denver area. According to the plea agreements, between 10 April 2020 to 31 March 2021, the two (2) controlled a series of businesses in a strip mall in Colorado.

The women received the proceeds from the drug activity typically in large currency amounts and as part of their operation, before transferring the money to Mexico, they would divide the funds into smaller increments to evade various reporting and identification requirements imposed by money service businesses. According to court documents, from 10 April 2020 to 28 January 2021, drug trafficking proceeds transferred through the businesses totalled between US$3.5m and US$9.5m.

One of the defendants was sentenced to twenty-four (24) months for ML related to a drug trafficking operation, while her co-defendant was sentenced to seventy-two (72) months in federal prison for conspiracy to commit money laundering.

According to the ruling, these defendants took part in a multi-million-dollar money laundering and drug trafficking operation that was shut down because of excellent work by the investigating partners at the Internal Revenue Service (IRS) Criminal Investigations and the Drug Enforcement Administration (DEA).

READ MORE

https://www.justice.gov/usao-co/pr/two-thornton-women-sentenced-money-laundering-related-denver-area-drug-trafficking

MANAGING RISK ASSOCIATED WITH CASH INTENSIVE BUSINESSES

- *Identifying cash intensive businesses*

The FATF requires financial institutions assess the ML and TF risks relating to customers, countries or geographic areas, products and services, and delivery channels. These institutions are expected to implement policies and procedures to identify higher-risk relationships at on boarding. Cash intensive businesses are considered to present a heightened level of ML/TF risk, due to the receipt of large amounts of cash. These businesses span a number of sectors/industries such as gas stations, supermarkets, beauty salons, restaurants, car washes and retail stores. While most of these businesses conduct legitimate business, some aspects of their operations are susceptible to ML or TF. It is therefore important that LFIs understand the nature of customers' business operations, the intended use of the account, anticipated transaction volume, products, and services required and the geographic locations involved in the relationship.

- *Ongoing Monitoring*

Ongoing monitoring is a critical element of the LFIs AML/CFT/CPF Program. LFIs are required to implement a framework, to facilitate the ongoing monitoring of customer transactions and accounts, to validate that the business activity of cash intensive businesses, is consistent with the nature of the operations of the business. The systems and controls should be capable of identifying suspicious or unusual transactions.

- *Independent Testing*

In order to ensure that risk management systems and internal controls in relation to cash intensive businesses are in place and are operating effectively, LFIs are required to establish and implement an independent testing framework. The framework should allow for testing to ensure that LFIs are effectively identifying cash-intensive businesses and monitoring their activities to identity potential suspicious activities.

RANSOMWARE- HOW TO FIGHT BACK!

Ransomware is a form of malware that encrypts a victim's files and demands a ransom or payment to restore access to the data upon payment.

A ransomware attack is a clear and present danger that poses significant risks to individuals and organisations. Ransomware has significantly increased in sophistication and frequency. The most significant contributor to the sudden recent spike in ransomware attacks, was the dramatic shift from a linear attack model to a multi-dimensional Ransomware as a Service (RaaS) model.

RaaS is a subscription based business model that provides access to ransomware to those with little or no experience. It has been hailed as one of the primary reasons for the rapid proliferation of ransomware attacks worldwide.

Paying a ransom to the threat actor is generally NOT a recommended practice. There is no guarantee that you will get what was promised and one should not provide any economic incentive that would allow these criminals to carry out future attacks.

An organisation would also not want to gain a reputation as being a 'payer' in the cyber world, as this will make them more of a target in the future. From an organisational perspective, it is critical to have an implemented incident response plan as well as a ransomware playbook in place, so that one can respond quickly and efficiently in the face of a ransomware attack.

A ransomware attack can cause severe disruption to an organisation's operations and reputation. When faced with a ransomware event, responding appropriately is essential to containing and minimising the damage. By the time an organisation is aware of mass encryption it is often too late, as encryption and demanding a ransom are the last phases of a breach. Despite this, it is still possible to contain and potentially even stop some parts of an attack.

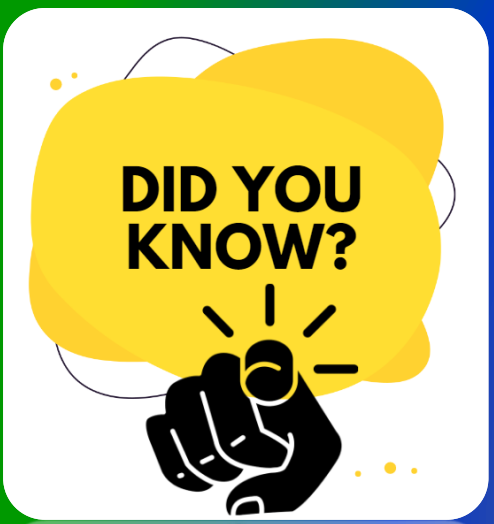
The following recommendations are provided as initial steps that individuals and organisations can take to help prepare for and possibly prevent a ransomware incident:

3. Endpoint antivirus solutions should be the initial mechanism deployed to all users across the enterprise. Monitor all endpoint connection requests and establish validation processes.
4. Proactive end-user education and training are critical in helping to prevent compromises of all types. This can be achieved through employee training and building a cyber-awareness programme that senior management actively champions.
5. Ransomware attacks rely heavily on the threat actor's ability to steal the credentials of those accounts. One of the best defence measures against ransomware is multi-factor authentication (MFA). MFA can decrease the ransomware risk as it requires an additional level of authentication.
6. Monitor the security posture of all your vendors to prevent third-party breaches.
7. Organisations should apply the least privilege methodology to file access on enterprise networks as ransomware targets common user files on local computers and on network shares. Once least privilege is in place users should be granted only the minimal permissions necessary for them to function in their job role.
8. Implement a robust vulnerability and patch management process. This should include proactive monitoring and remediation throughout the enterprise.

1. Avoid clicking on questionable links. Phishing scams do not only occur via email; malicious links can also be accessed via web pages.
2. Implement backup management policies and procedures that will ensure that the appropriate back-up measures are implemented to protect information system resources from loss or corruption, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

A layered approach to IT security is important as it helps to reduce the impact of a ransomware attack before it happens.

In a case where a ransomware attack has already occurred, a defensive approach gives the enterprise a wider scope of action towards remediation since they need to possess an awareness of the collated data, giving them the ability to devise the best mitigation strategies possible. Such a strategy will entail making user authentication more resistant to attacks, immediately detecting and removing any threats and lastly being in a position to roll back any actions taken by attackers. One thing for certain is that ransomware is here to stay so it is up to IT professionals to continue the fight against it!



FinCEN identified a ransom trend of more than $5.2 billion in ransom payments made in Bitcoin, which is the most popular method of ransom payment demanded, due to the difficulty of tracing the transaction.

The US Department of Treasury Office of Foreign Assets Control (OFAC) issued sanctions against the Suex cryptocurrency exchange for facilitating ransomware transactions.

THANK YOU FOR YOUR SUPPORT AND COLLABORATION IN THE PAST YEAR. WE LOOK FOWARD TO A PRODUCTIVE AND PROSPEROUS 2023.

WE WISH YOU A

HAPPY NEW YEAR

FROM THE MANAGEMENT AND STAFF OF THE
FINANCIAL SECTOR SUPERVISION DEPARTMENT

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