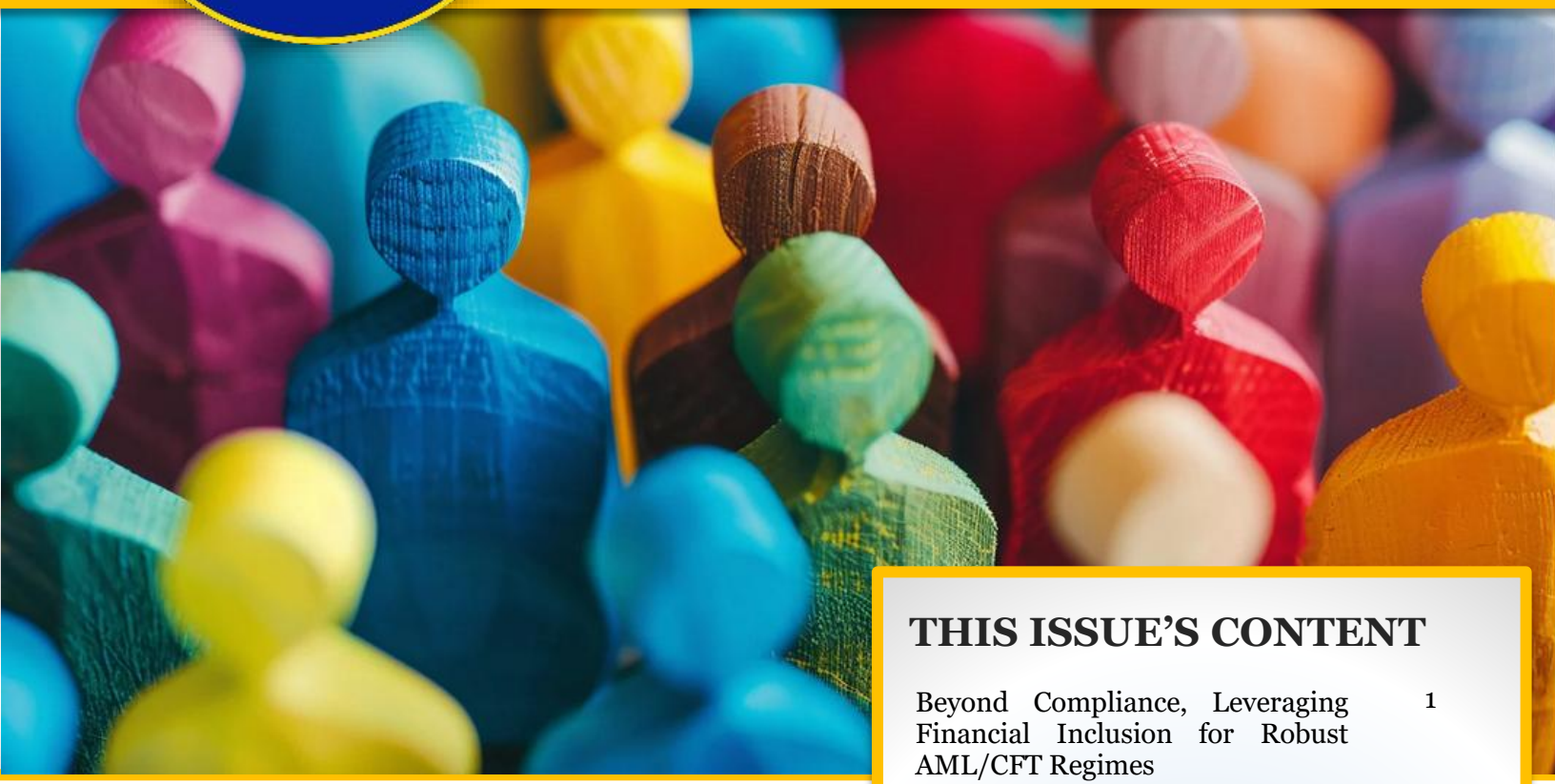
AML/CFT/CPF NEWSLETTER

ISSUE 17 JUNE 2025



THIS ISSUE'S CONTENT

BEYOND COMPLIANCE

LEVERAGING FINANCIAL INCLUSION FOR ROBUST AML/CFT REGIMES

By Annie Bertrand, Financial Inclusion Expert, United Nations Capital Development Fund (UNCDF)

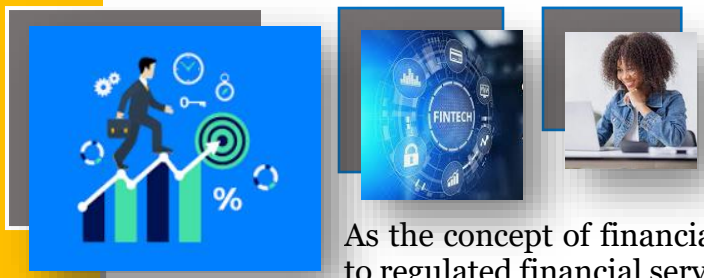
There are billions of individuals unbanked or underserved by the formal financial system, which makes their economic activities more vulnerable to exploitation, poverty traps, and crimes.

In June 2025, **the Financial Action Task Force (FATF) issued new guidance on financial inclusion** in response to the unintended consequences of its standards on developing countries.

The guidance highlights: "*Financial exclusion not only harms individuals and businesses, but can also represent a real risk to achieving effective implementation of FATF Standards by driving financial activities into unregulated channels*." Essentially, the FATF recognises that enabling access to formal financial services is no longer sufficient for integrity – countries must find ways to drive usage.

The definition of financial inclusion has been expanded to reflect the importance of essential aspects that must be addressed by countries:

> *"both **access** to and **active use** of an adequate suite of **regulated**, **appropriate**, **safe**, **convenient** and **affordable** financial services by individuals and entities that would benefit from such services*."



"*Appropriate*" means that the products/services are tailored to customers' needs and delivered transparently and fairly.

As the concept of financial inclusion evolves from merely providing access to regulated financial services to encompassing financial literacy, resilience, and the overall well-being of end-users, central banks around the world must increasingly complement their prudential role by actively fostering financial innovation that supports inclusive development.

To that end, the revised guidance provides multiple examples of how regulators can collaborate with financial institutions and financial technologies (fintechs) to develop new products that are better tailored to the diverse needs of different customers' profiles. Greater emphasis is placed on simplified customer due diligence in the implementation of the risk-based approach (RBA).

To reinforce the view that inclusion and integrity policy objectives are complementary, the FATF advises that: **"*where two or more measures would both effectively mitigate money laundering and terrorist financing (ML/TF) risks, the least burdensome option, having regard to financial inclusion, would typically be the most appropriate option.*"**

Such guidance implies a shift in the procedures of most financial institutions in the Caribbean.

In the Eastern Caribbean Currency Union (ECCU), the Eastern Caribbean Central Bank (ECCB) implemented multiple actions to accelerate progress. First, a Central Bank Digital Currency (CBDC) was piloted in 2023 to assess the feasibility of a digital wallet accessible to all citizens. Thanks to risk-based mitigation measures, simplified know your customer (KYC) procedures for on-boarding the DCash wallet enabled unserved citizens to participate in the digital economy.

Second, the banking legislation is being amended in the ECCU to make available to its citizens a basic bank account at no cost. These collaborative efforts between the ECCB and financial institutions are shining examples of initial bold steps that can significantly open access and drive usage of diverse financial products and services. Moreover, in 2022 the ECCB requested support from the United Nation Capital Development Fund (UNCDF) to strengthen its digital financial ecosystem. Through the European Union-funded *Digital Finance for Resilience (DF4Rez)* programme, the UNCDF partnered with various ECCB departments to deliver strategic technical assistance across five (5) areas:

CAPACITY BUILDING

UNCDF facilitated workshops and webinars to build regulatory capacity. A 2023 regional workshop in Trinidad and Tobago convened over one hundred (100) regulators, fintechs, and financial institutions to learn about global best practices in stimulating fintech innovation and streamlining the licensing and supervision process. In June 2025, a training session was delivered for ECCB staff and colleagues on fintech policies, with eighty-eight (88) highly engaged participants.

PAYMENT SYSTEMS LEGISLATION

UNCDF supported the drafting of the *Payment Systems and Services Bill* and regulations, which enables harmonised licensing and supervision of digital payment providers, including E-Money Issuers, across the ECCU. The legislation introduces regulatory "passporting", enabling licensed entities to legitimately operate across the eight (8) countries automatically. The economies of scale implied in this progress may have a catalytic impact on usage of digital financial services. UNCDF also provided technical assistance on risk-based supervision, agent oversight, and safeguarding of customers' funds.

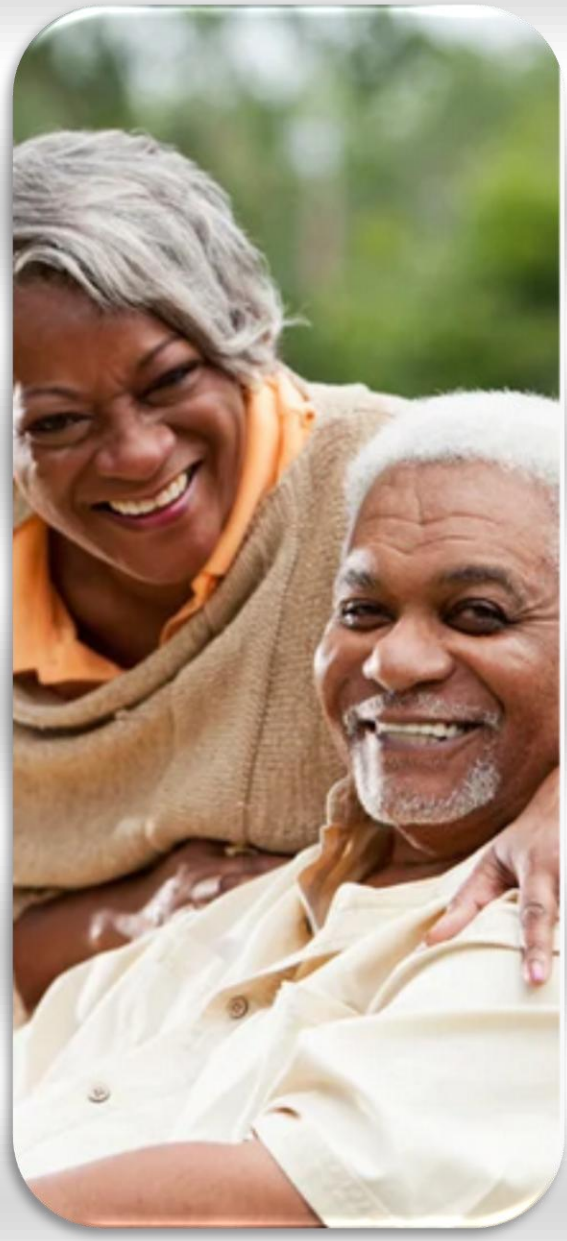
VIRTUAL ASSET SUPERVISION

With the Virtual Assets Business Act in place, UNCDF provided the Regulatory Oversight Committee with guidance to develop a supervisory framework for virtual assets, addressing emerging opportunities such as stablecoins and their implications for financial inclusion.

INTEGRATION OF CREDIT UNIONS TO THE ECACH

A recent legislative amendment across the eight ECCU member states has opened the Eastern Caribbean Automated Clearing House (ECACH) to credit unions, previously accessible only to commercial banks. This reform marks a pivotal step towards advancing digital financial inclusion in the sub-region, where forty-nine (49) credit unions serve over 400,000 members, representing an estimated 72.0 per cent penetration rate among adults. To operationalise this opportunity, the Caribbean Confederation of Credit Unions partnered with the ECACH to assess the feasibility of connecting credit unions' core banking systems and payment channels to the ECACH network. With funding from UNCDF, a pilot initiative is underway to integrate four (4) selected credit unions into the ECACH system in 2025.

A key priority identified is the development of guidelines to promote greater use of simplified customer due diligence and expand the RBA, balancing anti-money laundering and combating the financing of terrorism (AML/CFT) compliance with the imperative of advancing financial inclusion across the region.



In conclusion, financial inclusion strengthens AML/CFT regimes by enhancing traceability, transparency, and accountability. It shifts transactions from cash-based anonymity into formal financial channels that can be monitored and governed. At the same time, it enables regulators to focus oversight where it is most needed - on high-risk actors - while expanding access for the unbanked and underserved populations.

As the mandate of financial regulators continues to broaden, substantial investments are required to strengthen their capacity, not only to foster financial innovation, but also to ensure that market actors effectively manage risks. In the years ahead, their role will only become more critical and complex, making the adoption of a proportional approach to supervision more important than ever. Given the scale of both the challenges and opportunities, I hold deep respect and admiration for their work, and it has been a privilege to support their efforts across the region.

REGULATORY UPDATES

APPROVAL OF COMPLIANCE OFFICERS IN SAINT LUCIA

1

On 27 May 2025, the ECCB issued a circular to Licensed Financial Institutions (LFIs) in Saint Lucia outlining the procedure for the approval of a Compliance Officer. This follows the enactment of the Money Laundering (Prevention)(Amendment) Act No 18 of 2024, which amended Section 16 of the Money Laundering (Prevention) Act Cap 12.20 (MLPA) of Saint Lucia.

The circular detailed the new requirements introduced by the amendment and refers to the Compliance Officer's roles and responsibilities as defined in Regulations 22-26 of the Money Laundering (Prevention) Regulations (MLPR) 2023. According to Regulation 25(1) of the MLPR, the Compliance Officer must be "*independent, accountable and reports directly to the Board of Directors on the compliance function*." The Compliance Officer also serves as the central point of contact for both the ECCB and Financial Intelligence Authority (FIA).

Under the revised Section 16(1)(n) of the MLPA, LFIs are required to appoint a Compliance Officer at the management level who is fit and proper, and approved by the ECCB in consultation with the FIA. The ECCB also provided guidance on the implementation of these provisions, which took effect 1 June 2025.

THE EUROPEAN UNION (EU) REMOVES JAMAICA AND BARBADOS FROM THE HIGH-RISK MONEY LAUNDERING LIST

2

On 10 June 2025, the European Commission announced an update to its list of high-risk jurisdictions with strategic deficiencies in their AML/CFT regimes. Jamaica and Barbados were removed from the list, having demonstrated significant progress in strengthening their AML/CFT regimes. No other Caribbean countries were delisted at the time. The changes will take legal effect following a scrutiny and non-objection period by the European Parliament and the Council of the European Union (EU), which is expected to conclude within a period of one (1) month.

READ MORE

https://finance.ec.europa.eu/news/commission-updates-list-high-risk-countries-strengthen-international-fight-against-financial-crime-2025-06-10_en

3

HIGH-RISK JURISDICTIONS SUBJECT TO A CALL FOR ACTION - 13 JUNE 2025

On 30 June 2025, the ECCB issued a circular to LFIs, following the FATF's advisory dated 13 June 2025. The advisory highlighted jurisdictions with significant deficiencies in their AML/CFT/CPF frameworks. The FATF called on its members and other jurisdictions to apply counter measures when dealing with the following countries.

1. Democratic People's Republic of Korea (DPRK)

The FATF remained deeply concerned by the DPRK's failure to address significant AML/CFT deficiencies and the ongoing threat posed by its illicit proliferation-related activities. LFIs are required to:

- Terminate correspondent relationships with DPRK banks;
- Close any DPRK banks or subsidiaries operating within their jurisdictions; and
- Limit business relationships and financial transactions with DPRK individuals and entities.

2. Iran

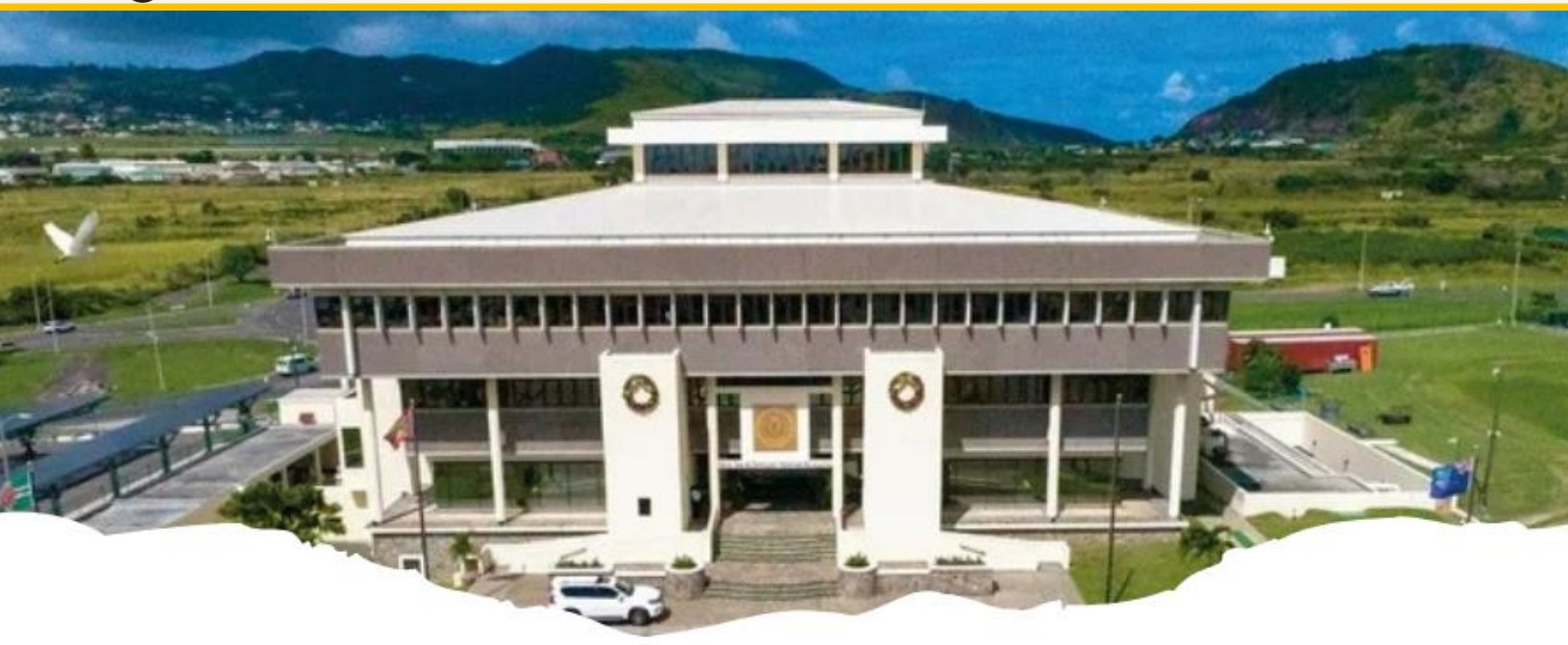
Iran committed in June 2016 to address strategic deficiencies but had not completed all required actions as of February 2020. As a result, it remained listed under the FATF's Call for Action until full implementation of its Action Plan.

3. Myanmar

In February 2020, Myanmar committed to address its strategic deficiencies. Myanmar's action plan expired in September 2021. The FATF set a deadline of October 2025 for corrective measures, after which it would consider imposing countermeasures. LFIs must apply enhanced due diligence when engaging in transactions or business relationships involving Myanmar.

READ MORE

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-june-2025.html



ECCB IN ACTION

Strengthening Safeguards, Advancing Compliance

Keeping you informed on what the ECCB is doing to combat money laundering, terrorist financing and proliferation financing

PRESENTATION AT REGIONAL COMPLIANCE SUMMIT

The ECCB participated in the Annual Regional Compliance Summit held in the Commonwealth of Dominica on 24 and 25 April 2025. The conference was co-hosted by the Dominica Cooperatives Societies League Ltd, and the Financial Services Unit under the theme: *Shaping the Future of Compliance in the Region*. The ECCB presented on day two of the event, on the topic "***The Future of Compliance in the Caribbean***". The event was well attended with over one hundred (100) participants from commercial banking, credit union, insurance, designated non-financial business professionals and offshore banking sectors.

STRENGTHENING COMPLIANCE: AML/CFT/CPF TRAINING FOR FINANCIAL SECTOR PROFESSIONALS IN ANTIGUA AND BARBUDA

On 21 May 2025, the ECCB, in collaboration with the Office of National Drug and Money Laundering Control Policy (ONDCP), conducted an AML/CFT/CPF training session at the Financial Services Regulatory Commission Training Room in St John's, Antigua. As part of the session, the ECCB delivered a focused presentation on AML/CFT Governance, emphasising the importance of strong oversight and effective compliance frameworks within financial institutions.

Other key areas covered during the training included Customer Due Diligence, Ongoing Monitoring, and Suspicious Activity Reporting. The session was attended both in-person and virtual by professionals from the banking and credit union sectors.

ECCB HOSTS FINANCIAL CRIME RISK ASSESSMENT TRAINING

The ECCB, as part of its ongoing efforts to strengthen financial crime compliance, hosted a two-day training on money laundering, terrorist financing and proliferation financing (ML/TF/PF) risk assessments. The sessions, which were held on 2-3 June 2025, were led by Dr William Scott-Grob, Director of Research and Analysis at the Association of Certified Anti-Money Laundering Specialists (ACAMS).

The training aimed to equip participants with a comprehensive understanding of:

- The ML/TF/PF risk assessment lifecycle and its crucial role in a risk-based compliance framework.
- How to effectively integrate assessment findings into robust anti-financial crime programmes.
- The power of data, technology, and ongoing monitoring in driving informed, adaptive risk management.

Key topics covered during the training included:

- Understanding financial crime risks and the RBA.
- The pivotal role of ML/TF/PF risk assessments including methodologies and key drivers.
- Evaluating internal control effectiveness and assessing residual risks.
- Effective strategies for presenting assessment results and establishing a feedback loop for continuous improvement.

Participants included compliance department representatives from across the ECCU, as well as representatives from other ECCU national authorities.

SMISHING: THE GROWING THREAT OF SMS-BASED SCAMS

There are various forms of cybercrime committed by bad actors with nefarious intent. One prominent technique employed is **SMISHING.** The term Smishing is an amalgamation of the terms **SMS** (Short Message Service) also known as text messages, highlighting the medium where the attacks perpetrated, and **Phishing** which is a technique employed by criminals to deceive individuals to produce sensitive data such as usernames, passwords, PINs and other private data.

MAJOR ELEMENTS OF SMISHING

Malicious website links: cybercriminals may use deceptive links that direct users to fake websites designed to mimic legitimate ones. The fraudulent sites often prompt users to enter their credentials, which can result in the installation of malware on the user's device or the theft of sensitive data.

Social engineering: Attackers use manipulative techniques, such as persuasive language and a strong sense of urgency, to make their messages appear credible and trustworthy. These tactics are intended to trick users into taking actions that compromise security.

COMMON SMISHING STRATEGIES

False Invoices – Messages are sent to inform the recipient that they have been charged for an item or service. These are designed to prompt the recipient to click on a link in an attempt to clarify what appears to be an erroneous or unauthorised transaction.

Lottery Scams – Messages claim the recipient has won a lottery or prize. They typically include a link to a fraudulent website that requests personal information under the guise of verifying the winners' identity or processing the prize.

Bank Account Alerts – Messages state that suspicious activity has occurred on the recipient's bank account. A link, purporting to be from the bank, is provided to "resolve" the issue, but instead leads to a phishing site designed to steal login credentials or personal data.

Package Tracking Notifications – Scammers impersonate reputable courier services, sending messages that a package is in transit, delayed, or requires action. These messages include links to fake tracking sites aimed at collecting sensitive information from the recipient.

PROTECTION OF CUSTOMERS FROM SMISHING

- Educate customers on the bank's official contact channels and communication methods (example verified phone numbers, email addresses, and website links).
- Encourage customers to verify the legitimacy of any sender's address and, or phone number before clicking on links or responding, especially when communication was not initiated by the customer.
- Advise customers that if in doubt, they should contact the bank directly using official contact details to confirm the authenticity of the message before taking any action.

INCREASE IN WIRE TRANSFER FRAUD: A GROWING THREAT TO FINANCIAL INSTITUTIONS

By: Ms Lennique Quashie, Manager - Financial Analysis Unit, ONDCP-Antigua and Barbuda

Criminals are no longer fixated on breaching your systems; they're targeting your clients!

Wire Transfer Fraud is rising sharply across financial institutions, driven by a surge in sophisticated cyber-enabled fraud (CEF) schemes. Recent analysis of Suspicious Activity Reports (SARs) reveals a troubling uptick in the exploitation of email systems and online banking platforms to move funds, regionally and internationally, without authorisation.

At the core of this crime typology are Email Account Compromise (EAC), Business Email Compromise (BEC) and social engineering tactics such as smishing. Unlike traditional hacks, criminals are not *"breaking in;" they are being let in*.

These attacks do not target your network firewalls; they weaponise the trust your institution has built with clients throughout the entire business relationship. By manipulating this trust, criminals gain unauthorised access to your products and services.

HOW? They impersonate you to your clients and your clients to you!

They hijack online banking platforms and legitimate email threads, then issue fraudulent wire transfer instructions that closely mimic past communication. These instructions often appear authentic, making them difficult to detect in real time. On the client side, success hinges on deception: your account holders being ***tricked by subtly altered or spoofed emails, phishing links, calls or texts notifications and requests that appear to come from your institution.***

Accordingly, the fallout is profound: unauthorised cross-border transfers, regulatory scrutiny, significant loss of client funds and most critically, reputational damage through the erosion of clients' trust.

So, what should you do?

ACTUAL CASE

WIRE TRANSFER REQUEST

YourClient appeared to request a US $130,000.00 wire transfer to **NewVendor**.

INSTRUCTION APPROVED

The email looked routine, familiar language and known contacts, and the transfer was processed.

Verification? None

INSTRUCTION DENIAL

Days later, **YourClient** denied ever sending the instruction.

SPOOFED AND LOST

YourBank's internal investigation revealed: a spoofed email, systems intact, client's trust breached, restitution demanded, funds gone.

RECALL ATTEMPT FAILED

Attempt to retrieve funds was unsuccessful.

SAR FILED

Suspicious Activity Report to FIU was two weeks late.

Some institutions may consider withholding reports of such incidents.

However, the financial and reputational cost of not reporting is far greater.

The threat is therefore no longer purely technical; CEF is behavioural. Institutions **MUST** re-learn their clients' habits, spot anomalies and implement airtight procedures. Focus must be placed on patterns, context and client behaviour to strengthen the institution's defences.

Tools Follow Rules, But Procedures Set the Rules!

Key Mitigation Strategies:

✓ **Elevate Verification Protocols**

1. **Use What is Secure and Take It Offline, When Needed:** If a request appears unusual or inconsistent with a client's typical behaviour, pause and go offline; call the client directly. Always verify wire transfer instructions using pre-established contact methods, not those provided in the suspicious email. Criminals count on your team choosing what's convenient over what's secure! Be alert to:
   a. Slight domain variations (e.g., maryjane@xyz.com vs maryjaane@xyz.com).
   b. Unusual formatting, spelling errors and changes in timing, tone, nature or urgency.

2. **Flip The Model:** It is not practical to call every client, so flip the model. Keep a pre-authorised beneficiary list and require clients to notify you before any transfer to new beneficiaries. This proactive step can drastically reduce fraudulent instructions.

3. **Treat Self-Initiated Wires as High-Risk:** CEF is no longer the exception; it is a prevailing crime typology. Transfers initiated via **online banking platforms**, especially those involving new beneficiaries **or unusually large amounts**, **must be treated with enhanced scrutiny**. Therefore:
   a. Implement a two-step or call back verification process that relies on secure information known only to you and your client.
   b. Set hard thresholds to enable dual approval of transfers above a defined limit.

✓ **Know Your Client; Know What's Normal**
Use customer history to define what is abnormal. Flag instructions to new beneficiaries, sent at odd hours, from new devices, or through unusual channels. If something feels off, it probably is.

✓ **Use The Intelligence**
Law enforcement or Financial Intelligence Units' (FIU) directives, advisories, typologies and sector specific guidance are powerful tools, but only if you read, discuss and implement the recommended actions.

✓ **Educate Your Clients**
Proactive education is part of your first line of defence. Let clients know what to expect from you, and what not to trust. Remind them to safeguard passwords, avoid phishing and smishing links and "if they did not expect it", call YOU first.

✓ **Train Your Staff**
Equip your team to understand and detect CEF, both completed and attempted. Remember, use all available information to reinforce learning.

✓ **Report Almost Immediately!**
All attempted or successful attacks must be reported to your FIU with supporting details to prevent undue analysis delays. Filing SARs late diminishes their investigative value, hinders law-enforcement ability to recover any funds and exposes your institution to serious sanctions.

In today's digital age, Wire Transfer Fraud is no longer rare, it is routine. Your institution's defences lie in unwavering awareness, strong procedures and constant vigilance.

One click. One compromised credentials. One unverified instruction. Thousands can be lost.

Put the right safeguards in place now, because the next transfer you process could be fraudulent!

AI: A GAME CHANGER FOR WORK, BUT WHAT ARE THE RISKS?

By the Management Information Systems Department

Artificial Intelligence (AI) can be defined as the science of creating intelligent machines that generate outputs for a given set of human-defined objectives. As AI continues to evolve from mere data processing (traditional AI) to data creation (generative AI), it is becoming increasingly integrated into various aspects of our lives in transformative and efficiency improving ways. While we enjoy these improvements, we must accept that the use of AI introduces noteworthy risks that must be carefully managed. Success in AI risk management depends on how well we balance innovation with the responsibility to safeguard privacy, and many experts believe that organisations are not balancing these paradigms effectively enough. This article helps the reader in this balancing act.

Microsoft reports that three (3) out of four (4) professionals utilise AI at work, and 30.0 per cent report saving time through the use of AI and automation tools, according to IBM. AI systems learn and continuously improve over time from new data and experiences, making them useful in many environments. Employees can leverage AI's ability to quickly and accurately process large amounts of data to save time by automating tedious and repetitive tasks, to improve data-driven decision-making, communication, data entry and analysis, and many more mundane tasks. These real-world applications of AI lead to an increase in productivity as it allows individuals to focus on more high-value, complex and strategic tasks.

Awareness of the risks associated with the use of AI is of equal importance as the benefits. It is imperative to develop a culture of caution when using this technology in the workplace and to be cognizant of the associated risks. AI poses privacy risks as it collects and uses data which can be leaked in a cyber-attack. This raises significant ethical and legal concerns as sensitive and personal information can be exposed, infringing on individual privacy rights.

AI systems can also have detrimental effects if a false positive or false negative is generated as part of an AI automated decision–making process. For illustration purposes, consider the panic and wasted resources that could result from an AI enhanced cybersecurity platform incorrectly categorising a threat as benign. On the other hand, failure to correctly identify an active threat leaves an environment vulnerable to attack, as there will be no action taken towards mitigation.

Additional risks to consider arise from the quality of data. Since AI systems are trained on historical data, their performance is directly tied to the quality of that data. Therefore, if the training data is incomplete or lacks diversity, the AI system may generate inaccurate or fabricated responses, commonly referred to as 'hallucinations.' Furthermore, since much of the data used to train AI models reflects historical trends, it often carries inherent biases.

These biases can then be reflected or even amplified in the AI's outputs, leading to skewed or unfair results.

These examples illustrate that the risks associated with use of AI are dynamic and this makes it challenging for organisations to develop risk mitigation strategies. The ambiguous and sometimes absent standards for identifying, understanding and measuring AI-related risks, are also testing the limits of existing risk management capabilities. In the face of these challenges, the following can help organisations to develop a culture of caution for AI use:

- Handle data input into AI systems with caution; avoid disclosing sensitive or confidential information.
- Always double-check AI-generated results before using them.
- Avoid over-reliance on AI.
- Regularly audit and monitor AI systems.
- Implement robust cybersecurity controls such as data privacy and security, data classification and AI usage policies to safeguard the AI infrastructure.
- Continuously educate employees and provide relevant updates as AI rapidly progresses.
- Create, review and update policies and procedures to manage the use of AI in the organisation.
- Employ stricter data anonymisation and encryption techniques
- Implementation of Data Loss Prevention (DLP) solutions to limit the exposure of sensitive data.

As AI continues to evolve, many companies are increasingly experimenting with its applications; whether as standalone technologies or embedded in existing applications to realise transformative benefits. These benefits are not without exposure to flaws and risks. Organisations are encouraged to reap the full benefits of AI by maintaining a balance between innovation and caution. When we navigate AI's potential with caution, we will benefit from its power to enhance productivity while mitigating the risks that come with it.

References

1. What is artificial intelligence (AI)? ISO. [Online] [Cited: 10 31, 2024.] https://www.iso.org/artificial-intelligence/what-is-ai.
2. Matzelle, Emily. Top artificial intelligence statistics and facts for 2024. CompTIA Community. [Online] 2 29, 2024. [Cited: 11 7, 2024.] https://connect.comptia.org/blog/artificial-intelligence-statistics-facts#:~:text=Impact%20of%20AI%20on%20Jobs%20and%20the%20Employment%20Market&text=IBM%20reports%20that%2030%25%20of,the%20emergence%20of%20new%20jobs..
3. Ai at work: It's time to embrace ai. Oracle. [Online] [Cited: 10 1, 2024.] https://www.oracle.com/us/products/applications/oracle-ai-at-work-report-5037501.pdf.
4. Esperanca, Hugo. Ai in workplace - balancing opportunities and risks. Collaboris. [Online] 8 15, 2024. [Cited: 11 7, 2024.] https://www.collaboris.com/ai-in-workplace-opportunities-and-risks/.
5. Ai at work is here. now comes the hard part. Microsoft. [Online] [Cited: 11 7, 2024.] https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part#:~:text=75%25%20of%20knowledge%20workers%20use,work%20more%20(83%25).

WELCOMING OUR NEW AML/CFT INTERN

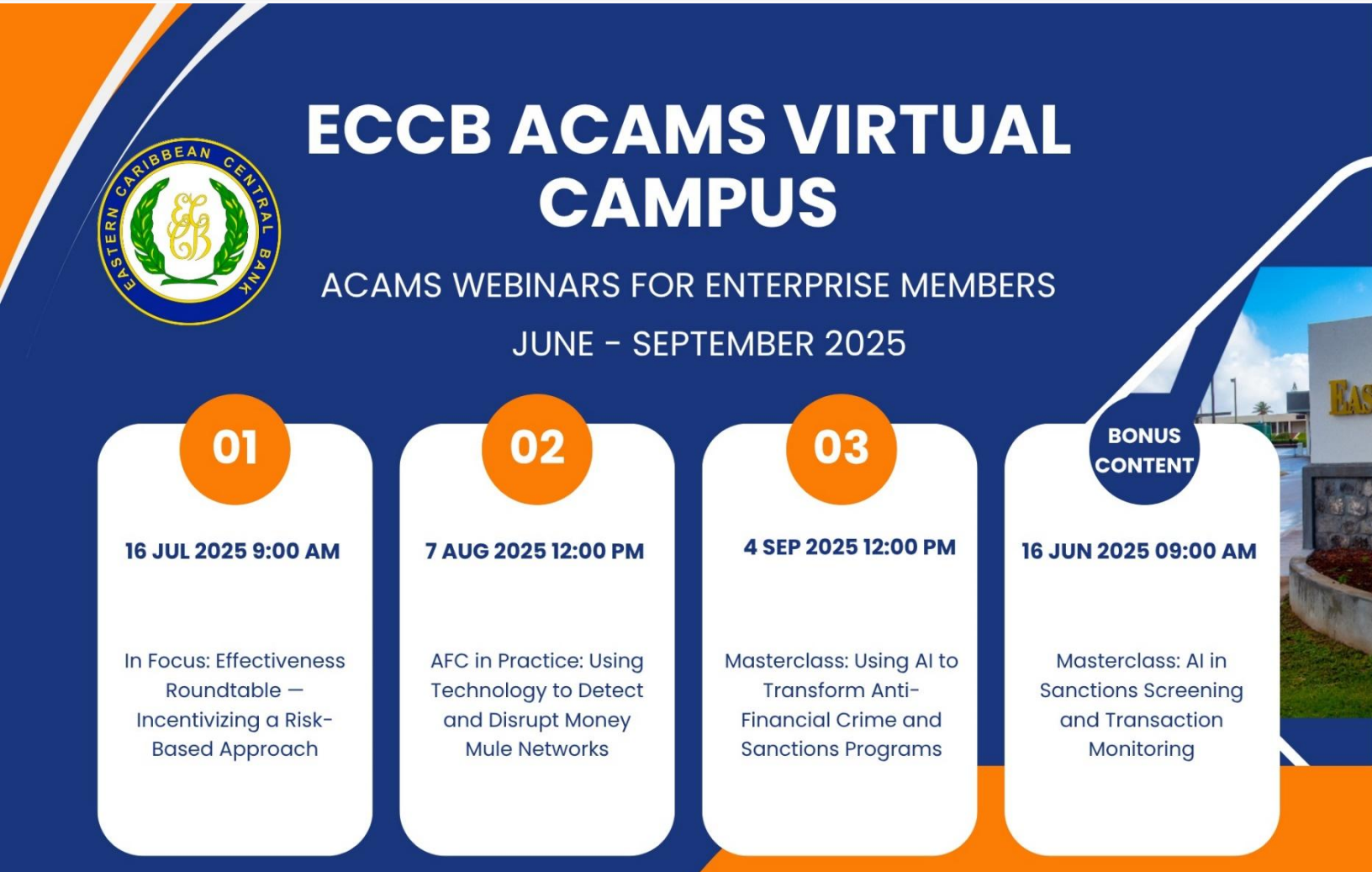
We are thrilled to welcome **Agassi Moreau** to our team as an **AML/CFT Examiner Intern**!

Agassi brings over eight (8) years of experience in loss prevention and a strong foundation in crime prevention to his new role. He holds a Bachelor of Laws from the University of London and a Master of Laws in International Commercial Law from the University of Salford, Manchester, where his research focused on strengthening regulatory frameworks for Citizenship by Investment programmes and improving due diligence practices.

Agassi is a Certified Anti-Money Laundering Specialist (CAMS) and a member of the Association of Certified Fraud Examiners (ACFE). He is currently attached to the AML Supervisory Unit of the Financial Sector Supervisory Department.

We are excited to have Agassi's knowledge and experience to contribute to our ongoing efforts in advancing our AML/CFT/CPF initiatives.

Please join us in giving him a warm welcome!



Have you read the previous issues of the AML/CFT/CPF 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) 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