



# AML/CFT/CPF NEWSLETTER

ISSUE 14 SEPTEMBER 2024

## THE USE OF ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

*Applications, Considerations, and mitigation strategies*

Advances in big data, cloud computing, machine learning and the increasing demand for digital products has set the stage for the adoption of Artificial Intelligence (AI) in the financial sector. To date, various forms of AI technologies have been integrated into the global financial system. This article examines the role of AI in the financial sector, discusses the associated ethical considerations, and outlines strategies for ethical deployment of AI.

## THIS ISSUE'S CONTENT

The Use of Artificial Intelligence in Financial Services	2
Regulatory Updates	5
New and Emerging Money Laundering Techniques	7
Non-Traditional Predicate Offenses to Money Laundering	9
Understanding Nominee Arrangements – Part 2	11
Typology – ECCB's Advisory on Job-Search Scams	12
Reflecting on an AML/CFT Stalwart	14

# APPLICATIONS OF AI IN FINANCIAL SERVICES

The financial services sector is undergoing significant transformation driven by AI's ability to gather vast amounts of data and the ability to process this information. Below are some key ways that AI is reshaping the industry:



## Regulatory Applications

The automation and data analytics capacity of AI can be leveraged by financial institutions to meet regulatory obligations more efficiently.

**AML/CFT Compliance** - AI-powered data analysis allows institutions to efficiently identify high risk alerts and to allocate resources accordingly, to better manage transaction monitoring. It also facilitates essential customer due diligence and enhanced due diligence tasks, by continuously comparing identity documents to other forms of identification and risk-relevant data.

**Fraud Detection** – Fraud detection systems now actively learn and adapt to new security threats. These systems monitor transactions for irregularities, flagging suspicious activities for investigation.

**Regulatory Compliance** – Financial institutions can leverage AI to identify and update relevant policies and procedures in keeping with advancements in AML/CFT legislature, enhancing the efficiency and accuracy of reporting, thus improving regulatory compliance. Additionally, AI can lower the risk of non-compliance by comparing customer profiles, banking products and services to regulatory requirements on an ongoing basis.

**Risk Management** – AI supports risk mitigation by analysing data to manage operating accounts, capital adequacy, liquidity positions, market risk, and credit risk.

**Stress Testing** - AI can improve the analysis of complex balance sheets and stress testing models, enabling financial institutions to meet regulatory stress testing requirements.



# APPLICATIONS OF AI IN FINANCIAL SERVICES

## CONSIDERATIONS

Licensed financial institutions (LFIs) must carefully consider the ethical implications of deploying AI technologies to ensure fairness, security, and compliance. Responsible implementation is essential to avoid unintended consequences and maintain trust among stakeholders.



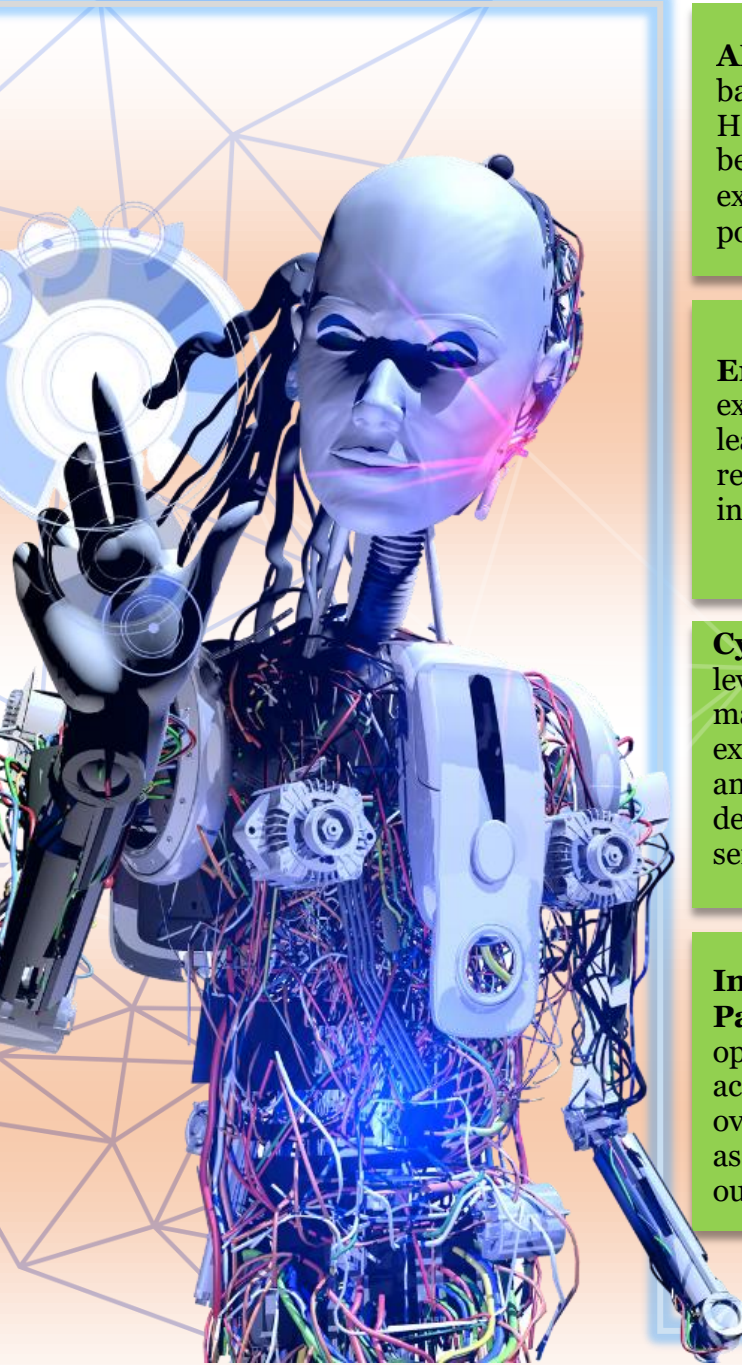
### Considerations for LFIs when implementing AI Systems

**AI and Data Quality** – AI technologies rely on a well-defined base code, as well as extensive data mining to operate effectively. However, sourcing high-quality data to build this base code may be challenging. Additionally, the base code might oversimplify or exclude elements of the domestic market and customer behaviour, potentially resulting in the generation of unpredictable outcomes.

**Embedded Bias** – AI technologies, could exacerbate financial exclusion, social inequity and reinforce misplaced biases as the learning process is dependent on mining data. This data may be reflective of unjust historical patterns, as well as inaccurate information.

**Cyber Security/Data Protection** – Malicious actors may leverage AI technologies to create convincing phishing emails or malware, targeting financial institutions to steal important data or execute ransomware attacks. The capacity of AI to unmask otherwise anonymous data also raises concern regarding privacy breaches, as decisions undertaken by AI systems could inadvertently leak sensitive information used during training of the AI systems.

**Increased Operational Risk and Dependence on Third-Party Providers** – Technical failures in AI systems can heighten operational risk in financial institutions. Additionally, high acquisition costs of personnel with the necessary expertise to oversee the internal development, management, and risk assessment of an AI solution, often leads to excessive reliance on outsourcing, creating additional vulnerabilities and dependencies.



# APPLICATIONS OF AI IN FINANCIAL SERVICES

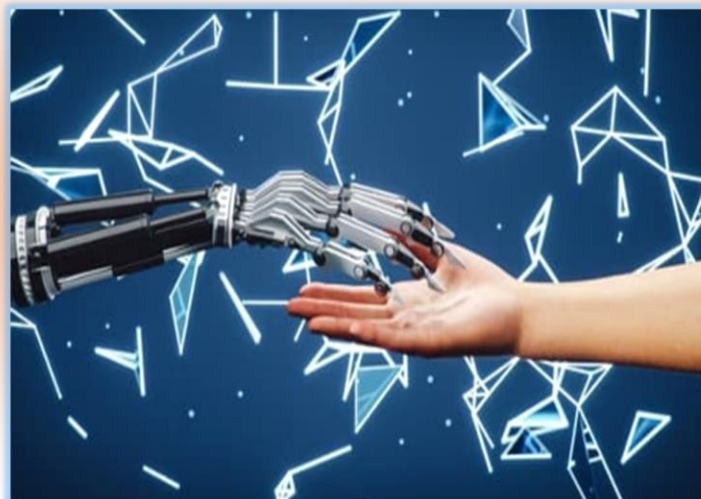
## MITIGATION STRATEGIES

To ensure the ethical deployment of AI technologies, LFIs should consider the following measures:

**Robust AI Governance Framework** – LFIs should establish a framework outlining clear guidelines, policies and procedures which define the roles and responsibilities for AI oversight and ethical use. This framework should include a culture of risk awareness, risk mapping and ongoing money laundering and terrorist financing risk assessments as integral components of AI governance.

**Effective Data Management** – The base model data should be reviewed to ensure data quality and accuracy. To facilitate risk assessments in the areas of ethical and regulatory compliance, as well as the application of tools for identifying and reducing undesirable biases, where necessary, it is imperative that every action in the lifecycle of the AI being deployed, be documented.

**Capacity Building** – LFIs should recruit talent with the requisite skills to ethically deploy and regulate AI solutions. LFIs should also conduct ongoing training and upskilling of employees on AI governance, with targeted training provided for employees directly involved in the development and application.



**Operations Management** – LFIs should stay updated on research and industry developments on AI management, and ensure that robust contingency plans exist in the event of a technical failure. They should also periodically analyse the base code and training data against AI decisions to evaluate and mitigate potential bias in algorithms.

**Understanding Human Influence** - Prior to deployment, LFIs should thoroughly understand the AI's base code and source data, input-output processes and various users of the technology to ensure transparency. AI decisions should also be validated by a human, and this requirement should be explicitly stated in the institutions internal control policy.

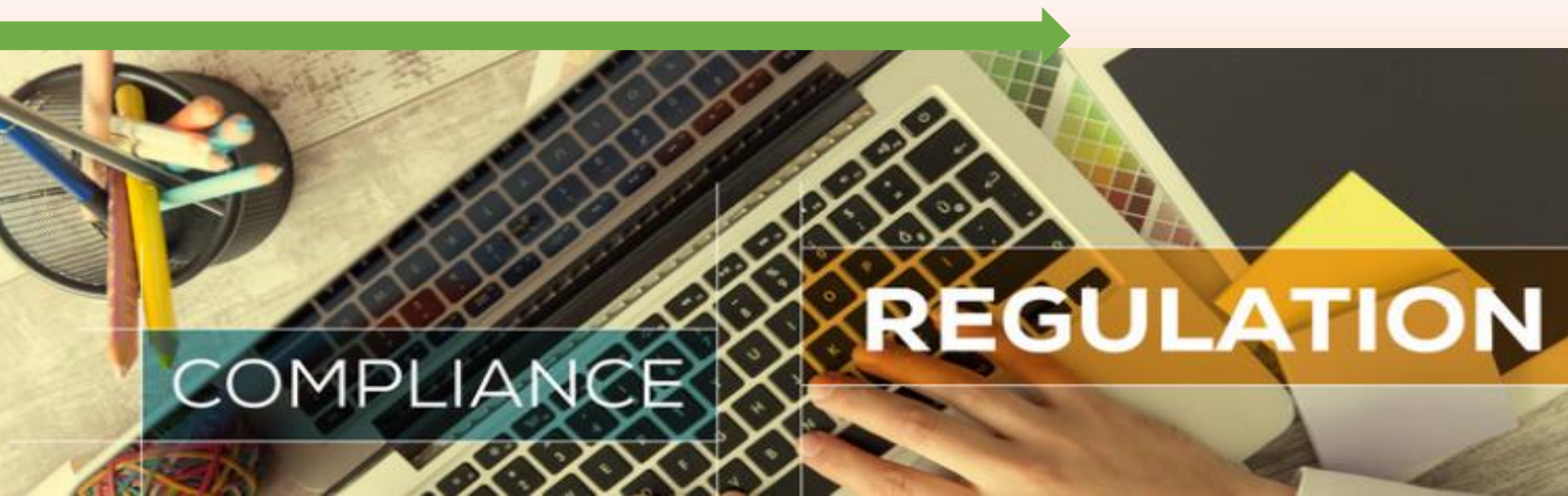
**Monitoring and Reporting** - To guarantee adherence to legal requirements, ethical considerations, and regulatory standards, institutions should conduct routine internal and external audits of AI systems. They should also consider monitoring AI performance in real-time, highlighting bias, irregularities, or deviations from expected behaviour, reporting any significant issues to the relevant authorities.

## Conclusion

The adoption of AI technologies continues to transform the financial sector, improving customer experiences, credit decision-making, and supporting robust corporate governance. Nevertheless, these advancements also introduce a range of inherent risks and challenges that must be carefully understood and managed. It is crucial for institutions to evaluate the benefits and drawbacks of implementing these technologies, and develop deployment strategies tailored to their unique needs and risk appetite.



## REGULATORY UPDATES



## ANTIGUA AND BARBUDA ISSUED UPDATE TO MONEY LAUNDERING AND THE FINANCING OF TERRORISM GUIDELINES – MAY 2024

In May 2024, Antigua and Barbuda has issued an update to its Money Laundering and the Financing of Terrorism Guidelines for Financial Institutions (MLFTG). The update addresses the following:

### 1. Period Review of Customer Information –

Amendment to Part 1 Paragraph 2.1.10 to insert the prescribed time frame for updating customer due diligence information based on the risk posed by the customer as follows:

Customer Risk	Review Period
High	1 year
Medium	3 years
Low	5 years

The update also includes the due diligence information which must be considered when conducting the reviews.

### 2. Transparency and Beneficial Ownership of Legal Persons and Arrangements

The MLFTG was updated to include guidance on the identification and verification of beneficial ownership of legal persons, legal arrangements and other structures capable of exercising beneficial control. The guidelines include the application of a multi-prong approach to beneficial ownership – Ensuring that the beneficial ownership information is **adequate, accurate and up-to-date**.

[READ MORE](#)
[Antigua and Barbuda MLFTG-Guidlines-for-FIs-Update-21-May-2024.pdf](#)

## FATF RAISES CONCERNS OVER GAPS IDENTIFIED IN AML/CFT MEASURES FOR GATEKEEPERS

The Financial Action Task Force (FATF) warned that countries such as the United States of America (USA), China and Australia can unwittingly or wittingly, facilitate high-level of corruption by failing to subject attorneys, real estate agents and other “gatekeeper” professions to anti-money laundering requirements as identify in the FATF Recommendations. This was concluded following the ‘*Horizontal Review of Gatekeepers*’ which was published on its website as at 8 July 2024.

According to the report the FATF has undertaken this horizontal review to assess the current state of play and identify areas that FATF members must prioritise for further improvement. The report highlighted that the USA, Australia and China had zero per cent scores, for failing to implement any of the FATF's standards for the gatekeeper businesses and professions. There were some positives, with more than half the nations surveyed scoring better than 80.0 per cent with the average score around 74.0 per cent. Portugal and Luxembourg were the best performers with a perfect score of 100.0 per cent, having met all of the FATF's technical recommendations for Designated Non-Financial Businesses and Professions (DNFBPs).

The requirements of the FATF Recommendations on gatekeepers including conducting customer due diligence, implementing internal controls, and providing a supervisor with adequate powers to conduct risk-based supervision—are critical requirements to address the vulnerability of gatekeepers to money laundering and corruption threats. As such, the FATF urges members that have not yet implemented the FATF recommendations with regards to gatekeepers, to take immediate action towards implementation.



<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Gatekeeper-TC-Corruption.html>

## **SANCTIONS AGAINST TERRORISM: COUNCIL RENEWS THE EU TERRORIST LIST AND DESIGNATES A NEW ENTITY**

The Council of the European Union (EU) has decided to add the entity “*The Base*” to the EU Terrorist List as at 26 July 2024. The Base is a white supremacist and neo-Nazi accelerationist paramilitary group and training network, formed in 2018 by Rinaldo Nazzaro 2018.

3

The sanctions that will apply to “*The Base*” include the freezing of its funds and other financial assets or economic resources in EU member states. It is also prohibited for EU operators to make funds and economic resources available to the organisation. These sanctions were effective as at 26 July 2024.

The Council also renewed the list of persons, groups and entities subject to restrictive measures with a view to combatting terrorism, delisting one deceased person and maintaining the rest. There are currently 15 persons and 22 groups and entities subject to the restrictive measures in force.

The EU terrorist list was first adopted in December 2001 in the wake of the terrorist attacks on 11 September of that year.



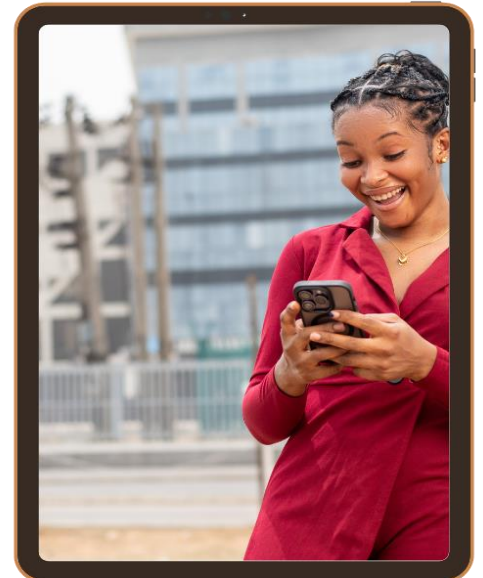
<https://www.consilium.europa.eu/en/press/press-releases/2024/07/26/sanctions-against-terrorism-council-renews-the-eu-terrorist-list-and-designates-a-new-entity/>

# New and Emerging MONEY LAUNDERING TECHNIQUES

## Social Media and Influencer Marketing:

Using influencers to promote products or services that can be overvalued, allowing for the laundering of funds through inflated sales.

The rise in social media and influencer marketing has created novel avenues for money laundering. A trend has been observed in which criminals exploit social media influencers to promote products or services that are artificially inflated in value, facilitating the laundering of illicit funds through inflated sales. This technique leverages the massive reach and trust that influencers have with their audience to create a false perception of demand for a product or service.



*Social media influencers are individuals who have gained significant popularity and credibility on social media platforms, such as Instagram, YouTube, Tik Tok, Twitter, or Facebook. They leverage their large and engaged follower base to influence the opinions, behaviours, and purchasing decisions of their audience.*

In this scheme, a money launderer provides an influencer with a product or service to promote, usually a “luxury item,” that is priced well above market value and through sponsored posts, video reviews and endorsements. The influencer helps to promote the item making it appear desirable or exclusive. As a result of this interaction, followers eager to emulate the influencer’s lifestyle, purchase the products or services at the inflated prices, believing them to be legitimate commodities which are in high demand.

Once the sale is completed, the launderer receives the payment, effectively “cleaning” the illicit funds by integrating them into the legitimate revenue streams of a high-demand business, such as restaurants, nightclubs, or casinos. This process can be repeated across multiple influencers and products, enabling criminals to launder significant sums under the guise of legitimate sales transactions.

The use of influencers for money laundering poses unique challenges for financial institutions, as the transactions often appear legitimate and are difficult to track. This is particularly challenging where cryptocurrency or online payment platforms are involved. As social media marketing continues to evolve, it is crucial for financial institutions to remain vigilant and implement appropriate monitoring systems to identify and mitigate emerging techniques, ensuring they are equipped to address new and evolving risks effectively.



## Non-Fungible Tokens (NFTs)

A Non-Fungible Token commonly referred to by its acronym NFT, is a token that is stored on a decentralised blockchain ledger that uses smart contracts to verify ownership. It is often stored on the Ethereum blockchain and vary in two significant respects from other digital assets:

1. Every NFT is distinct, non-fungible; and
2. A NFTs contains data linking it to a virtual or physical asset.



*Non Fungible means that an item is one of a kind and cannot be exchanged or replaced for an identical one. Common examples of NFTs are digital arts and photographs, collectibles, music, and games. Each NFT has a unique identifier which distinguishes one from the other.*

*Token refers to the digital certificate stored on the blockchain, proving ownership and authenticity.*

NFTs can be viewed as an irreversible digital certificate of authenticity and ownership for a particular asset. Similar to any other asset, NFTs can be utilised to facilitate money laundering (ML) as they possess value and are transferable. The following traits of NFTs make them appealing for ML:

- **Pseudonymous trading:** Ownership of NFTs is tied to cryptographic private keys, and not necessarily linked to a "real-world" identity.
- **Open access:** Although most transactions are processed by regulated marketplaces and exchanges that must conform to Know Your Customer (KYC) requirements, individuals can conduct transactions on public blockchains without verification.
- **High mobility:** NFT trades are not restricted by international borders. They can be transferred globally to anyone, at any time, without the need for inspection, customs examinations, or physical transportation and storage.
- **Price subjectivity:** Buyers' willingness to pay determines the value of NFTs. Due to this price subjectivity, money launderers may exploit the trading and sales of NFTs in a similar manner to physical art, transferring value through the payment of inflated prices for objects with artificially high value.

*Financial institutions should be aware of the characteristics of NFTs that make them attractive to money launderers and susceptible to misuse. When processing funds related to NFTs or engaging in their trading or sale, institutions must monitor transactions for suspicious activity and ensure that staff are trained to identify and address associated risks.*



# NON TRADITIONAL PREDICATE CRIMES TO MONEY LAUNDERING



Non-traditional predicate offenses have emerged as a significant contributor to money laundering schemes globally. They are considered to be those that are not traditionally known to be associated with financial misconduct, but can provide an avenue for illicit profit generation and concealment of funds. Risks related to the drugs trade, weapons of mass destruction, cash are globally well understood, however, there is need for increased awareness and focus on the non-traditional forms of ML. Let's explore two examples of non-traditional predicate offenses.

## ENVIRONMENTAL CRIMES

The Financial Action Task Force's (FATF) report on [Money Laundering from Environmental Crime](#) defines environmental crimes as criminal offences that cause harm to the environment. The report highlights that non-traditional environmental crimes such as illegal logging, pollution, and wildlife trafficking carry low risk with high reward, making them a lucrative and attractive source of revenue for criminals. The FATF report also indicates that fraud and misuse of shell and front companies are used to launder the proceeds of environmental crimes.

According to the FATF, environmental crimes are amongst the most profitable criminal activities in the world, generating approximately **USD 110 to 182 billion** annually.

The FATF emphasises that countries must recognise the proceeds from environmental crimes as a global threat. Accordingly, to mitigate the risks associated with environmental crimes financial institutions should allocate the necessary resources to identify and report suspicious activities associated with these crimes, and enhance coordination and cooperation with national agencies responsible for tackling these issues.

Similarly, a report published by the United Nations Environment Programme on '*Emerging Issues of Environmental Concern*', shows that the proceeds from environmental crimes are comparable in magnitude to those from other financial crimes. The World Bank's report on *Illegal Logging, Fishing, And Wildlife Trade: The Costs and How to Combat It*, estimates that governments lose between **USD 6 to 9 billion** annually in tax revenue due to illegal logging alone.



***Money laundering and environmental crimes trade pose a significant challenge to global security and sustainability.***

# COUNTERFEITING AND PIRACY-RELATED CRIMES

September 2024, Issue 14 | PAGE 10

## Intellectual Property Infringement

Intellectual property (IP) is no longer considered an emerging threat. IP plays a critical role in growth and innovation. The violation of IP ownership has emerged as a favoured method for laundering criminal proceeds, primarily because these tend to be overlooked as lower priority offenses. However, infringing products are no longer confined to counterfeit items like fashion apparel, luxury watches, and designer sunglasses. They now encompass an increasing variety of everyday goods, including food and beverages, pharmaceuticals, chemicals, electronics, and household items. These often subpar products can present serious health and safety hazards to consumers. Criminals are also capitalising on the lack of expertise by authorities in the subject area of IP, hence the inability to detect and determine the real value of IP.

## Illicit Trafficking of Counterfeit Good

The expansion and integration of the global economy provides tremendous opportunities for business growth. On the flip side unfortunately, this also creates an avenue for criminals to operate illicit trade networks and that includes illicit trading of counterfeit goods. In 2008, the Organisation for Economic Co-operation and Development (OECD) conducted a research into the economic impact on counterfeit and piracy.



The research found that international trade in counterfeit and pirated products was estimated at approximately USD 200 billion in 2005. In 2019, the volume of international trade in counterfeit and pirated products was estimated at USD 464 billion or 2.5 per cent of world trade. Illicit trade is not a victimless crime. Combating illicit trade is critical to mitigating its wide-ranging and far reaching diverse impacts, from exposing individuals to harmful products, to depriving governments of significant much needed tax income.

Increased public awareness is critical in mitigating the risk of counterfeit and piracy. Consumers also need to be made aware that piracy infringement and trafficking of counterfeit goods are criminal offenses.

## Addressing the Threat as Financial Institutions

1. Keep abreast with emerging ML/TF/PF risks and trends.
2. Monitor FATF updates to keep up to date with the list of designated predicate offences, as outlined in the FATF glossary.
3. Augment staff awareness programmes with emerging trends.
4. Adapt monitoring systems leveraging advance analytics and artificial intelligence to identify suspicious activities and trends.
5. Collaborate with local authorities in strengthening legal and regulatory frameworks.

***It is critical that LFIs ensure they do not accept funds derived from these predicate offences, as they would be considered proceeds of crime and may trigger legal and regulatory penalties.***



## Part 2: Understanding Nominee Arrangements

### Exploring the associated risks and mitigation strategies

Nominee directors, shareholders and similar arrangements play a crucial yet contentious role in global corporate frameworks. While legally permissible in many jurisdictions, they introduce significant regulatory challenges and pose money laundering, terrorist financing and proliferation financing risks, as they can be used to conceal the true beneficial owner of an entity, which necessitate proactive handling by national authorities and financial institutions. It is therefore important to understand the risks posed by such arrangements and to implement appropriate controls to mitigate these risks effectively.



#### Associated Risks

Nominee arrangements may be used to obscure the true owner of an entity, thereby creating a vehicle for tax evasion by concealing the beneficial owner. In such arrangements, the nominee may have no direct control or involvement in the entity, and their role is solely to facilitate the concealment of the beneficial owner. This arrangement is termed by the FATF as 'Signature for Sale'.

Moreover, as nominee arrangements obscure the true owner of an entity, aligning the assets to the beneficial owner can be challenging. These arrangements can also be used to facilitate the creation of complex structures with multiple layers, further complicating the identification of the beneficial owner.



#### Mitigating Measures

To mitigate the risks posed by nominee shareholders and arrangements, the FATF highlighted the importance of implementing the appropriate legislative framework to ensure transparency. This includes requiring nominee arrangements to be disclosed in the public registry, so that this information is readily available. Authorities may also consider prohibiting the use of such arrangements unless specific conditions are met, such as full declaration of the nominee and the purpose of the arrangement.



**It is essential for financial institutions to conduct due diligence on all parties involved in nominee arrangements,** applying enhanced measures where applicable and implement effective monitoring controls to promptly identify any ML/TF/PF risk exposure. Institutions should focus on understanding the terms of nominee agreements, including its nature, purpose, as well as the relationship between the nominee and nominator; particularly where politically exposed persons (PEPs) relationships exist. This thorough understanding will enable financial institutions to better assess and manage the associated risks, ensuring compliance with regulatory obligations and safeguarding against potential misuse.



**READ MORE**

<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf>



# ECCB JOB SCAM ADVISORY



The Eastern Caribbean Central Bank (ECCB) reminds Licensed Financial Institutions (LFIs) under the Banking Act, 2015, as amended, of advisory issued 05 September 2024 regarding the identified Job Search Scams proliferating across various Eastern Caribbean Currency Union jurisdictions.

## Key Observations

- 1 Victims are informed of their success in obtaining employment without any screening or interviews, and are required to provide personal information including banking details.
- 2 These scams typically promise unusually high wages for tasks such as typing, data entry, or correspondence preparation.
- 3 Victims receive payment for services via wire transfers or mobile transactions, followed by instructions to forward a portion of the received funds to third parties via money remitters.
- 4 Perpetrators avoid providing essential business details like company websites, social media pages, or physical addresses.
- 5 Phishing tactics are also employed, attempting to gain unauthorised access to personal devices and sensitive information.



**These scams are primarily targeting individuals interested in remote work opportunities or supplementary income through online platforms and social media channels.**

In response to this growing threat, LFIs under the Banking Act, 2015 as amended are urged to implement the following measures:

1

### **Risk Assessment**

- **Utilise** information, fraud alerts and advisories from relevant supervisory authorities, and law enforcement agencies, to stay updated on emerging threats.
- **Evaluate** instances of Job Search Scams involving your clients or clients of other financial institutions.

2

### **Reporting Obligations**

- **Adhere** to legal requirements mandating the reporting of all executed or attempted fraudulent activities related to Job Search Scams.
- **File Suspicious Activity Reports** promptly to relevant authorities, ensuring all pertinent information, including wire transfer information and relevant attachments, are accurately documented.

**LFIs are required to act in accordance with the advisory issued 05 September 2024.**



## **JOB SCAM ADVISORY**

3

### **Know Your Customer Practices**

- **KNOW** what is normal for your customer to better detect abnormal or suspicious activities.
- **DO** assess every transaction to determine a baseline, and scrutinise deviations. These include transactions above the established threshold, suspiciously large wire transfers and immediate withdrawals.

4

### **Employee Awareness and Training**

- Educate and update staff regularly on protocols and procedures for handling transactions potentially linked to Job Search Scams.
- Foster a culture of vigilance and prompt reporting of suspicious transactions.

# BEYOND THE OFFICE

## NEW CHAPTER FOR AN AML/CFT STALWART



**Derek Benjamin**

*Manager, Financial Compliance Unit,  
ONDCP, Antigua.*

“

*I would recognize the opportunity to foster mutual profession respect with industry colleagues, most rewarding and gratifying.*

”

Mr Derek Benjamin started his career in AML/CFT/CPF supervision in 2006 as a Financial Analyst at the Office of National Drug and Money Laundering Control Policy (ONDCP), Antigua.

Mr Benjamin cited that having completed over twenty (20) years in the domestic banking sector and four (4) years in private enterprise, he decided to transition to a role within the public service as he envisioned at the time that it would have been less demanding ...Or so he thought!

In 2009, Mr Benjamin was appointed as Supervisor Financial Intelligent Unit. From 2015 to 2024, Mr Benjamin served as Manager of the Financial Compliance Unit. Mr Benjamin is excited to embrace the new chapter of life in retirement at the end of 2024.

Mr Benjamin is a firm believer that one should never pass on any opportunity for learning, no matter what that area of study may be. During his tenure in the AML/CFT field, Mr Benjamin obtained a certification in Risk Management for Increased Profitability and Cybersecurity Risk Management, Anti-Money Laundering and Financial Crimes Prevention Certification and became a trained Financial Action Task Force (FATF) Financial 3<sup>rd</sup> and 4<sup>th</sup> round assessor. Mr Benjamin also received training in Intelligence Gathering and Analysis, Law Enforcement, ML/TF/PF Risk Assessment and several other areas relevant to AML/CFT/CPF supervision.

The ECCB sat down with the AML/CFT stalwart to gain some insight into his rewarding career and notable contribution in the compliance space.

**Looking back on your career, what would you say have been the most rewarding moments or milestones?**

“When I joined the ONDCP, AML/CFT/CPF supervision was limited to the analysis of the statutory Annual AML/CFT Audit reports submitted by only a segment of the financial sector.



Consequently, we recognized the need for AML/CFT/CPF awareness in the financial sector.

This impelled me to initiate the development of a training and awareness campaign for regulated entities, under the guidance of our Legal Consul. This initiative led to the establishment of the Financial Compliance Unit, the Supervisory unit of the ONDCP.

Another fulfilling aspect of my career was the opportunity to forge excellent working relations with professionals within the financial service sector and colleagues within the regulatory and supervisory community. I would recognize the opportunity to foster mutual professional respect with industry colleagues as the most rewarding and gratifying aspects of my career. I would commend this concept of “mutual professional respect” as a guiding value for all professionals in this field.

**What would you say has been the exciting aspect of your career?**

I have always recognized that knowledge obtained should be used and shared. Consequently, I have found the recognition and invitation to share at local, regional and international forums as an AML/CFT/CPF subject matter expert as one of the more exciting and professionally rewarding aspects of my career.

“

*One should never pass on any opportunity for learning, no matter what that area of study may be.*

”

**Given your extensive experience in AML/CFT supervision, what advice would you give to professionals looking to pursue a career in this field, particularly to those new to the industry?**

To persons currently pursuing or aspiring to pursue a career AML/CFT/CPF supervision, here are my two pieces of advice:

1. Do not pass on opportunities for learning, whether they be directly or indirectly related to your immediate career path. No one can take back from you what you have already learnt.
2. Try to foster professional mutual respect with industry colleagues. It is only in working together, that effective supervision and oversight can be achieved.

The ECCB joins the ONDCP and the people of Antigua and Barbuda in celebrating and congratulating Mr Benjamin on his dedicated service and contribution to Antigua and Barbuda and the region.

As Mr Benjamin looks towards embarking on this new and exciting chapter, we wish him a happy and healthy retirement.



# ECCB AML VIRTUAL LEARNING CAMPUS

## ACAMS WEBINARS FOR ENTERPRISE MEMBERS



### ECCB AML VIRTUAL CAMPUS

#### ACAMS WEBINARS FOR ENTERPRISE MEMBERS

**OCTOBER - DECEMBER 2024**

**Start Date**

**OCTOBER**

12:00PM  
(DURATION 2 HOUR)

16

**Mandatory**

**AFC in Practice: Risk Assessing Politically Exposed Persons**

**Start Date**

**OCTOBER**

12:00 PM  
(DURATION 2 HOUR)

24

**Mandatory**

**AFC in Practice: Building Governance Frameworks and Management Reporting**

**Start Date**

**NOVEMBER**

12:00 PM  
(DURATION 2 HOUR)

21

**Mandatory**

**AFC in Practice: Automating Investigations and SAR filings**

**Start Date**

**DECEMBER**

12:00 PM  
(DURATION 2 HOUR)

12

**Mandatory**

**AFC in Practice: Using Technology and Statistical Tools to Fine-Tune AML Alerts**

**Bonus Content**

**Start Date**

**DECEMBER**

12:00 PM  
(DURATION 2 HOUR)

10

**Optional**

**AFC in Practice: Mastering Client Lifecycle Management**

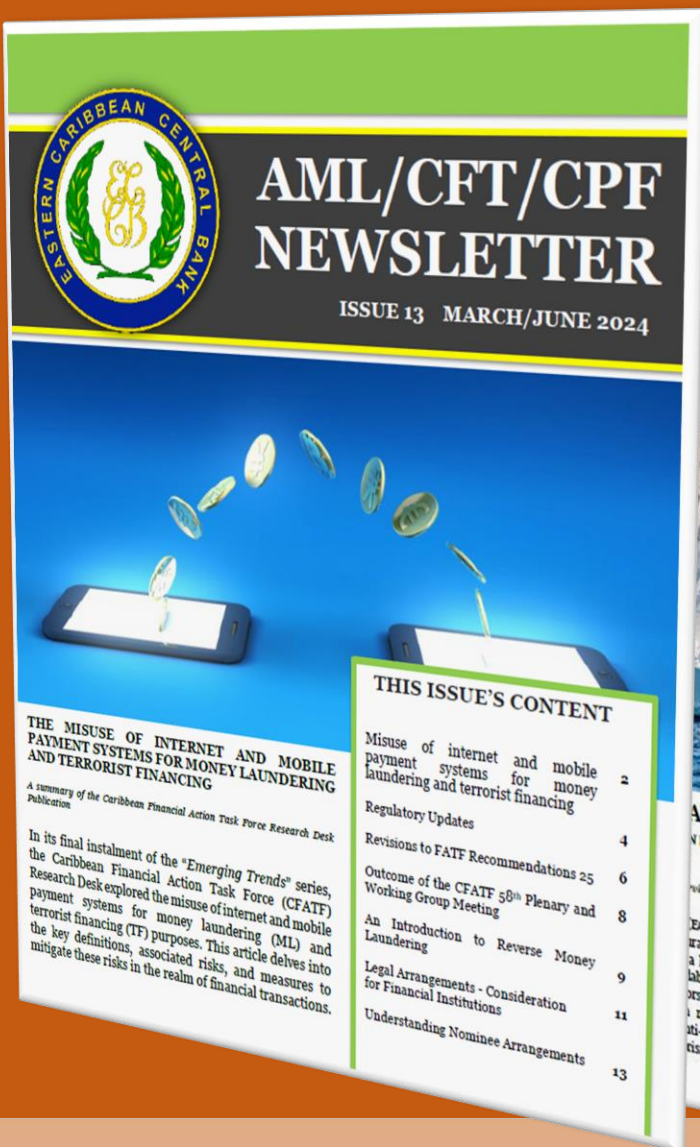
**FOR MORE  
INFORMATION**

Contact us at:

✉ [AMLSupervisoryUnit@eccb-centralbank.org](mailto:AMLSupervisoryUnit@eccb-centralbank.org)



*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) 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](mailto:AMLSupervisoryUnit@eccb-centralbank.org)**



@ECCBConnects



<https://www.eccb-centralbank.org/>



@ECCBConnects



Eastern Caribbean  
Central Bank