THE CENTRAL BANK OF BELIZE

MISSION

To promote the stability of monetary and financial systems for the wellbeing of Belize.

AML STRATEGY

It is the policy of the Central Bank of Belize (Central Bank) to contribute to the national AML strategy to prevent money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction.

This strategy is a collaborative effort between the Central Bank, other domestic and foreign supervisory authorities, and supervised institutions to actively identify, understand, and assess ML/TF/PF risks in Belize's financial system. Together, risk-based mitigating measures are implemented to align with international standards and best practices. In addition, on-going outreach is undertaken to sensitize stakeholders on AML matters.

CENTRAL BANK of BELIZE

Gabourel Lane
Belize City
BELIZE
Tel: (501) 223 – 6194
Web: www.centralbank.org.bz
Email: compliance@centralbank.org.bz

CENTRAL BANK of BELIZE

ANTI-MONEY LAUNDERING HIGHLIGHTS

Notice No. 1 | March 2025

MONEY LAUNDERING TYPOLOGIES

The Financial Action Task Force (FATF) Immediate Outcome 6 (IO6) requires countries to ensure that financial intelligence and other relevant information are appropriately used by competent authorities for money laundering (ML) and terrorist financing (TF) investigations.

In complying with these requirements, Belize's Financial Intelligence Unit (FIU) is responsible for reviewing and analyzing methods and trends related to ML/TF, commonly referred to as "typologies," to aid in ML investigations.

TYPOLOGIES IN BELIZE

An ML typology refers to a specific method, pattern, or technique used to disguise the origins of illegally obtained money. Several ML typologies were identified in Belize during the period 2017 to 2023:

- ❑ Embezzlement - *a type of financial crime, usually involving theft of money from a business or employer.*
- ❑ Fraud - *any activity that relies on deception to achieve a gain.*
- ❑ Structuring - *the act of splitting large sums of money into smaller transactions to avoid reporting.*
- ❑ Online phishing scams - *fraudulent attempts to steal personal information by pretending to be a legitimate entity online.*

PHISHING SCAMS IN BELIZE

Between March and August 2022, the FIU received multiple STRs from a financial institution about a growing threat: online phishing scams targeting Belizeans. These scams were organized and sophisticated, involving foreign scammers, harvesters, facilitators, and victims.

Here's what happened. Victims received emails that looked like official bank messages, asking them to click a link. Once they did, scammers gained access to their accounts and transferred funds to accounts controlled by recruited facilitators. Some funds were recovered, but money sent abroad was lost.

It was confirmed that phishing scams are increasing and pose a serious risk to Belize's financial system. In response, an awareness campaign was launched, including flyers, radio ads, and videos warning the public about phishing typologies.

This led to financial institutions reporting unsuccessful phishing attempts, proving that awareness and vigilance work.

Read about the typologies identified in Belize's MER at this link: https://www.centralbank.org.bz

HOW TO PREVENT, DETECT, AND ADDRESS ML TYPOLOGIES

FIs should consider the following best practices when addressing ML typologies:

- ❑ Determine how the typology impacts your products, services, customers, and delivery channels.
- ❑ Incorporate the assessment of new ML/TF trends or typologies into the risk assessment program;
- ❑ Update transaction monitoring systems to detect indicators linked to new typologies.
- ❑ Provide targeted training to ensure employees remain informed about new ML techniques and trends; and
- ❑ Revise Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Financing (AML/CFT/CPF) policies to reflect new and emerging risks from typologies.

KEY TAKEAWAYS

FIs are required to implement a robust AML compliance program, which includes, but is not limited to:

- ❑ Monitoring systems to effectively identify ML/TF/PF typologies;
- ❑ Training and awareness programs to empower employees to detect and prevent ML/TF/PF; and
- ❑ Report suspicious activity to the FIU.

Refer to the Central Bank's AML/CFT/CPF Guidelines at this link: https://www.centralbank.org.bz