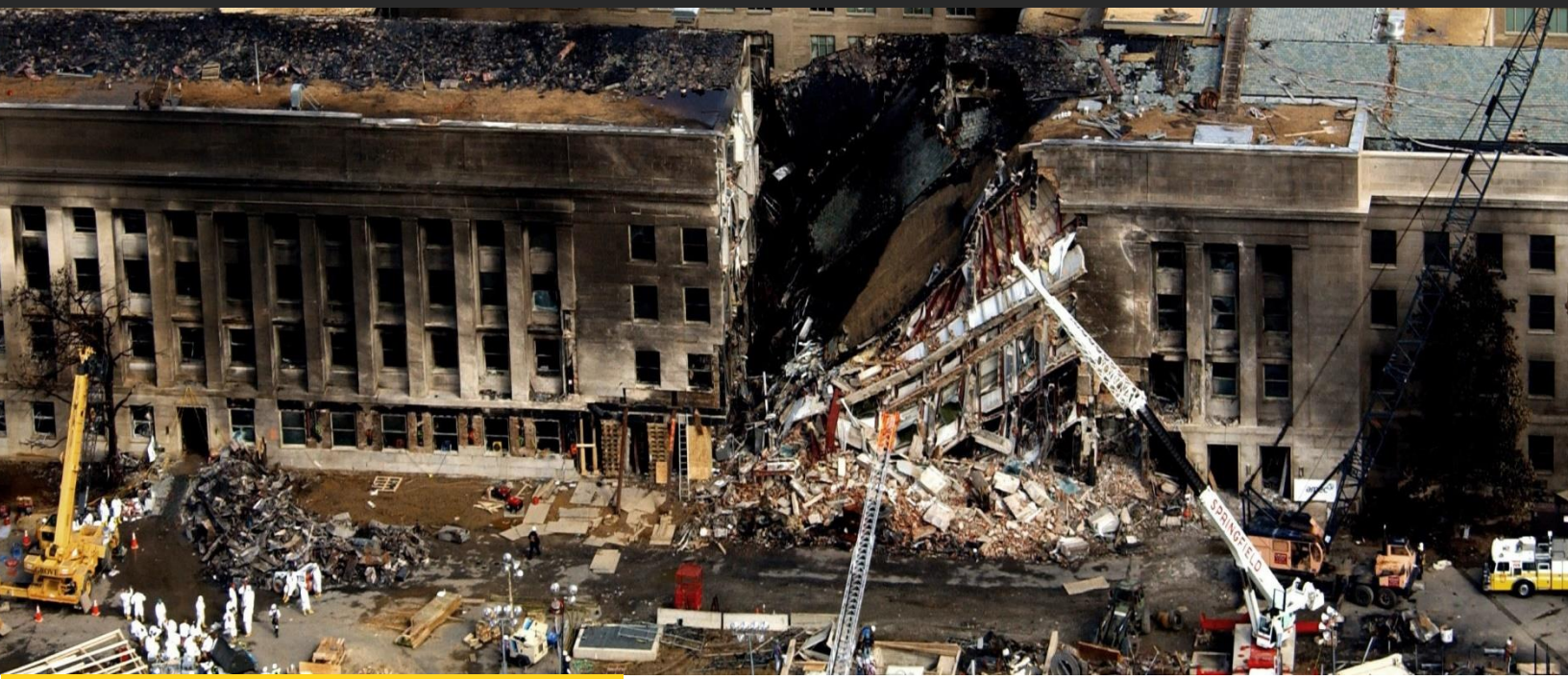
AML/CFT NEWSLETTER

ISSUE 3 SEPTEMBER 2021



THIS ISSUE'S CONTENT

TARGETED FINANCIAL SANCTIONS

Obligations of Financial Institutions

The Financial Action Task Force (FATF) Recommendations 6 and 7 require countries to comply with the United Nations Security Council Resolutions (UNSCRs or resolutions) relating to the suppression and prevention of terrorist financing (TF) and terrorism in addition to prevention, suppression and disruption of proliferation of weapons of mass destruction (WMD) and its financing.

These resolutions are the UNSCRs 1267 (1999) and the Al Qaida or Taliban sanctions regime, UNSCRs 1373 (2001) and any future UNSCRs which may impose Targeted Financial Sanctions (TFS).

Countries are required to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

Once implemented effectively, TFS can assist in protecting citizens from threats of WMD, terrorism and financial crime, by depriving proliferation financiers and terrorists use of their funds.

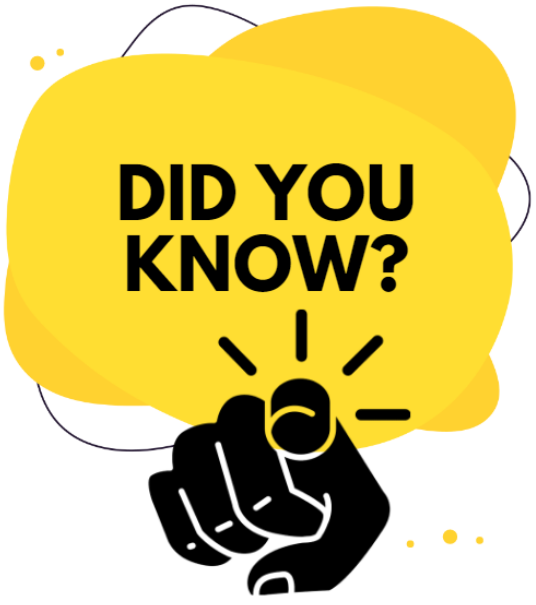
The United Nation's sanction requirements impose several obligations on financial institutions to include:

- Reporting to competent authorities, any assets frozen or actions taken in compliance with the prohibition requirements of the relevant resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities;
- Freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.
- Prohibition against financial services, funds and other assets being made available to or for the benefit of listed or designated parties;
- Prohibition against dealing with other assets and funds of a listed party or a designated person; and
- Implementation of policies, procedures and other systems of internal controls to facilitate the effective compliance with TFS.

The Eastern Caribbean Central Bank (ECCB), as the regulator and supervisor for licensed financial institutions in the Eastern Caribbean Currency Union (ECCU), has a mandate to maintain financial stability, by safeguarding the integrity of the financial sector. As part of this mandate, compliance with Anti-Money Laundering /Counter Financing of Terrorism (AML/CFT) requirements is imperative.

Recommendation 6: https://www.cfatf-gafic.org/index.php/documents/fatf-40r/372-fatf-recommendation-6-targeted-financial-sanctions-related-to-terrorism-and-terrorist-financing

Recommendation 7: https://www.cfatf-gafic.org/documents/fatf-40r/373-fatf-recommendation-7-targeted-financial-sanctions-related-to-proliferation



UN Security Council sanctions have taken a number of different forms, to include comprehensive economic and trade sanctions to more targeted measures, such as arms embargoes, travel bans, and financial or commodity restrictions?

The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation?

The Office of Foreign Assets Control (OFAC) Sanctioned Countries List as of 30 May 2021, include:

- **Cuba: restrictions on imports, exports, financial transaction and travel;**
- **Venezuela, Lebanon: restrictions on activities with specific parties;**
- **Iran: restrictions on imports, exports, and financial transactions; and**
- **North Korea: restrictions on imports, exports and travel?**

REGULATORY UPDATES

FATF: Opportunities and Challenges of New Technologies for AML/CFT

In July 2021, the FATF published a report on the Opportunities and Challenges of New Technologies for AML/CFT. The report focuses on ways in which new technologies may assist jurisdictions and regulated entities to become more effective in the implementation of AML/CFT Standards.

The report highlights the main advantages of new technologies to the private sector which includes:

- ✓ Better identification, understanding and management of money laundering (ML)/ terrorism financing (TF) risks;
- ✓ The ability to process and analyse larger sets of data in a more efficient and accurate manner;
- ✓ More efficient onboarding practices (digital);
- ✓ Achievement of greater auditability, accountability and overall good governance;
- ✓ Reduction in costs and maximising the allocation of human resources to more complex areas of AML/CFT; and
- ✓ Improvement in the quality of suspicious activity report submissions.

READ MORE https://www.fatfgafi.org/publications

FATF conducts second 12-month review of its Standards for Virtual Currencies and Virtual Asset Service Providers

On 05 July 2021, the FATF completed a second 12-month review of the revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (VASPs). The review assessed how jurisdictions and the private sector have implemented the revised standards, since the first 12-month review.

The second 12-month review revealed that while many jurisdictions and the VASP sector continue to make progress with the execution of the revised Standards on Virtual Assets and VASPs, the implementation was still insufficient.

READ MORE https://www.fatfgafi.org

Antigua and Barbuda Strengthens its AML Regulatory Framework

In July 2021, Antigua and Barbuda gazetted the amendment to its Money Laundering Prevention Bill No 9 of 2021, to enhance its regulatory framework. These include:

- ✓ Amendment to Section 2 thereby amending the definition of "money laundering offense" and inserting a new definition of "registration regulations".
- ✓ Amendment to Section 17, thereby laying out the conditions for who may not be eligible, or licensed to own or manage the business of a financial institution.
- ✓ Inserting Section 18E into the Principle Act to establish a general legal framework for registering unregulated institutions.

http://laws.gov.ag/

European Commission makes proposal to overhaul its AML/CFT legislation

On 20 July 2021, the European Commission presented an ambitious package of four (4) legislative proposals which aims to improve the detection of suspicious transactions and activities, and close the loopholes used by criminals to launder illicit proceeds or finance terrorist activities.

The new measures include:

- ✓ Establishing a new European Union (EU) AML Authority (AMLA Proposal) which will serve as the central authority coordinating national authorities, to ensure that the EU rules are consistently applied.
- ✓ A single EU Rulebook for AML/CFT for all members.
- ✓ Full revision of the EU AML/CFT for the crypto sector.
- ✓ An EU-wide limit of €10,000 on large cash payments.
- ✓ Amendment to its Third Country Policy.

Press Release: https://ec.europa.eu/commission/
Proposal : https://ec.europa.eu/finance/docs

TIPS FOR THE DETECTION AND SUBMISSION OF SUSPICIOUS TRANSACTIONS IN RELATION TO TF & PF

In order to be effective, measures to address ML/TF/ Proliferation Financing (PF) risk must be implemented and enforced in practice. The early detection and reporting of suspicious transactions is critical in the protection of financial institutions. Some tips to help facilitate the timely and effective reporting of suspicious activities include:

i. Implementing a risk-based AML/CFT/Counter Proliferation Financing (CPF) programme, with adequate and appropriate policies, procedures and systems of internal controls to mitigate inherent risks;

ii. Ensuring that staff are adequately trained in AML/CFT/CPF best practices and have access to updated sanctions list;

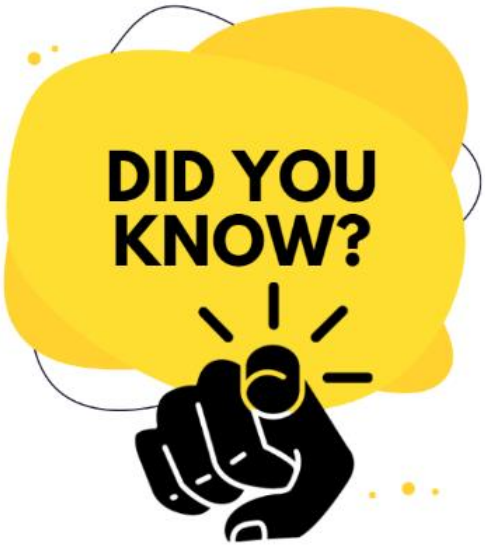
iii. Using transaction and surveillance monitoring tools as part of the AML/CFT/CPF risk management framework during on-boarding and for ongoing monitoring;

iv. Having a sound knowledge or understanding of the relevant laws, regulation and guidelines relating to TF and PF;

v. Ensuring that all clients are screened against the relevant sanctions lists during the on-boarding stage, before establishing relationships and on an ongoing basis;

vi. Being familiar with TF and PF red flags and indicators; and

vii. Understanding who needs to file a suspicious transaction report, to whom and the reasons for filing.



All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction?

MITIGATING PROLIFERATION FINANCING THROUGH EFFECTIVE CUSTOMER DUE DILIGENCE MEASURES

The COVID-19 pandemic has forced banks and other financial institutions (FIs) to innovate amidst uncertainty and other challenges. While the pandemic has negatively impacted some industries, others have capitalised on opportunities for growth and survival through innovation. In a parallel movement, criminals (to include proliferators) have also adjusted their enterprise in order to advance their mission. Though not a new concept, increased focused is now placed on the exploitation of the financial system to facilitate WMD.

Recent typologies have indicated that designated persons and entities continue to explore new ways to evade TFS, regardless of the geographical proximity to proliferating states.

For example, they may arrange complex financial transactions and/or shipments, passing through countries that have weak ML/TF/PF controls.

The FATF defines WMD proliferation as the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual use goods, used for non-legitimate purposes). As such, the financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD.

One may question why is PF relevant to the ECCU? In order to obtain the various components to manufacture WMD, proliferators need access to formal banking systems and embark on trade activities to support their illegitimate activities. This does not preclude the ECCU region. The role played by banks and other FIs is therefore vital in the fight against PF.

FATF Recommendation 1 requires that FIs identify, assess, understand and mitigate their PF risks. Institutions may do so within the framework of their existing compliance programmes, and are not expected to establish duplicative processes for PF risk assessment or mitigation.

Financial institutions must develop a clear understanding of the contextual information and the sources of PF risks that they are exposed to, and take appropriate measures to mitigate these risks, in accordance with AML/CFT legislation. The nature of risk mitigation measures implemented will depend on the source and degree of risks identified.

Institutions must implement TFS without delay. This requirement is not risk-based, but rather rule-based.

International best practices recommend that FIs incorporate changes in United Nations designations into their monitoring and surveillance system without waiting for national transposition or communication.

The key elements of a CPF program are very similar to that of an AML or CFT program. Institutions are required to have:

- A robust onboarding processes for customers to include verification of beneficial ownership;
- Effective procedures for sanctions screening to identify sanctioned individuals and entities; and
- Transaction monitoring systems to identify suspicious activities.

As part of the due diligence process, FIs are required to establish procedures for obtaining and verifying the identification of a customer or account holder, at the onset of a business relationship. Policies and procedures must be implemented to ensure that information obtained at the on-boarding stage is accurate and remains relevant throughout the relationship.

The customer due diligence (CDD) process should be risk-based. Measures should be employed to establish the identity of the owners of legal entities with whom the institution has established business relationships. Understanding the nature of the business, including, products or services provided, and the ownership and control structure is imperative. Verification of beneficial ownership should be through the use of relevant data, information and documentation obtained from reliable sources.

FIs are required to screen the names and addresses of customers against the consolidated list of designated persons and entities (including entities owned or controlled by them) published by the UNSC.

Other lists which can be used for sanction screening purposes include, but is not limited to:

- ✓ The US Consolidated Sanctions List;
- ✓ OFAC- Specially Designated Nationals (SDN);
- ✓ The EU Consolidated Financial Sanctions List;
- ✓ Consolidated List of Financial Sanctions Targets in the UK (Office of Financial Sanctions Implementation HM Treasury);
- ✓ UK Sanctions List (Foreign, Commonwealth & Development Office); and
- ✓ Interpol Wanted List.

Technology remains a key enabler in the effectiveness of identifying financial crime risk through screening, more efficiently and on a real-time basis. It is therefore recommended that institutions employ sanction screening tools to assist in the screening process.

It is imperative that persons involved in the sanction screening process are suitably trained, knowledgeable, supervised and that the appropriate levels of quality control and assurance are in place to ensure compliance.

Customer activities should be monitored for significant changes, inconsistencies in transaction patterns and to ensure that records remain updated. In applying a monitoring program, institutions must consider monitoring by transaction type, frequency, amount, geographical origin/destination and risk profile. Increased monitoring of accounts for customers identified as high risk should be conducted to ensure the transaction activity is in keeping with the stated purpose.

In such cases it would be appropriate to apply enhanced due diligence measures such as, obtaining additional information on the customer, reviewing and updating of customer's information periodically or as required by the relevant regulations. Also, understanding the intended nature of the business, being reasonably satisfied with the purpose of the transaction, and establishing and taking measures to verify the source of funds and wealth are critical.

In conclusion, banks and other FIs are encouraged to make the necessary adjustments to their compliance programs to include appropriate PF controls. The only way to combat proliferation is through the disruption of the financial flows available to procure the illicit goods, services and technology required for the development of WMD.

CASE STUDY

RIGGS BANK: THE PRICE PAID

Riggs Bank (Riggs/ the bank) was usually referred to as the "bank of presidents" and was a traditional linchpin in the United States' (US) financial community. The bank operated as a brokerage house in 1836 and provided depository and chequing services dating back to 1840. It established banking relationships for about 95.0 per cent of all embassy accounts in Washington. However, within three (3) years, things went terribly wrong for the bank.

Questions to consider: What were the issues? Could your institution face the same fate?

Riggs & Pinochet

It is reported that Augusto Pinochet, the former dictator of Chile held a total of twenty-eight (28) accounts at Riggs, spanning 25 years (earliest account opened in July 1979) and totalling approximately US$8.0 million. A Riggs memorandum in 2002 stated that the value of the Chilean business at Riggs had *"average balances exceeding $100 million"*. During a routine regulatory examination of Riggs's International Private Banking Department in April 2002, Pinochet's accounts came to light. The bank failed to disclose the existence of accounts associated with a Politically Exposed Person (PEP), in response to a direct request by its regulators.

A senate report alleged that managers at Riggs had not only failed to comply with AML legislation but that they had actively aided Pinochet in laundering funds through offshore accounts and with altered account names. Additionally, accounts had been opened on Pinochet's behalf in the names of Ashburton Company Ltd. and Althorp Investment Ltd., both shell companies formed with the help of a Riggs offshore subsidiary. Pinochet's accounts were terminated, after the Office of the Comptroller of the Currency (OCC) raised serious concerns about the oversight of the accounts.

The OCC had three (3) main issues with the way Riggs dealt with the Pinochet accounts. These were:

1. The bank was of the opinion that Pinochet was no longer a PEP, choosing not to disclose his accounts when a request was made for a list of all PEP customers;

2. Failure to file suspicious activity/transaction reports when Pinochet moved large sums of money from accounts at Riggs to other foreign institutions. No disclosures were made about sums moved from the U.K and Spain ahead of attempts to seize Pinochet's funds by Spanish authorities; and

3. Lack of documentation on the source of the Pinochet's funds.

Riggs and Obiang

In 1995, Equatorial Guinea opened its first account at Riggs. This client became Riggs's biggest depositor with a balance of around US$700 million. Riggs held the Equatorial Guinea government treasury accounts, as well as the private accounts of President Obiang, his family and senior government officials. Some sixty (60) accounts were reported to have contained 'gifts' made to the leadership of the country by US oil companies.

Accounts held in the name of family members of President Obiang or in the form of related offshore shell companies, which had been established allegedly with the assistance of Riggs, had seen cash deposits of almost US$13 million between 2000 and 2003. In addition, large payments by oil companies were made directly into private accounts or accounts held by officials. After an investigation of the operations of Riggs was conducted, Mr Simon P. Kareri who served as the senior banker with responsibility for the Equatorial accounts, was fired in January 2004. The US Senate Report dated 14 July 2004, found that Riggs "had serviced the Equatorial Guinea accounts with little or no attention to the bank's AML obligations". It was apparent that Riggs had been aware of the proceeds of large scale bribery and corruption. The report also revealed that the bank, "exercised such lax oversight of the account manager's activities that, among other misconduct, the account manager was able to move more than $1 million from an account belonging to a ruling family member at Riggs to another bank for an account opened in the name of Jadini Holdings, an offshore corporation controlled by the account manager's wife."

The Saudi Arabian Diplomat Accounts

The allegations that triggered the initial investigation into Riggs by U.S authorities appeared in a Newsweek article in December 2002. The article indicated that a 'steady stream' of monthly payments had been uncovered which were credited to Omar Al Bayoumi, who had dealings with two (2) of the September 11th hijackers, namely Khalid Almihdhar and Nawaf Alhazmi. The money originated from the accounts of Princess Haifa Al Faisal, who was the wife of the former Saudi Ambassador to the U.S, Prince Bandar and daughter of the late King Faisal of Saudi Arabia.

In late November 2004, Saudi officials acknowledged that the Princess had given money to the family of Osama Basnan. The money, they claimed, was given as a donation towards medical expenses. Princess Haifa Al-Faisal was cleared of all allegations. The 9/11 Commission Report stated; "We have found no evidence that Saudi Princess Haifa al Faisal provided any funds to the conspiracy, either directly or indirectly."

The Results: Shareholder Suits and Fines

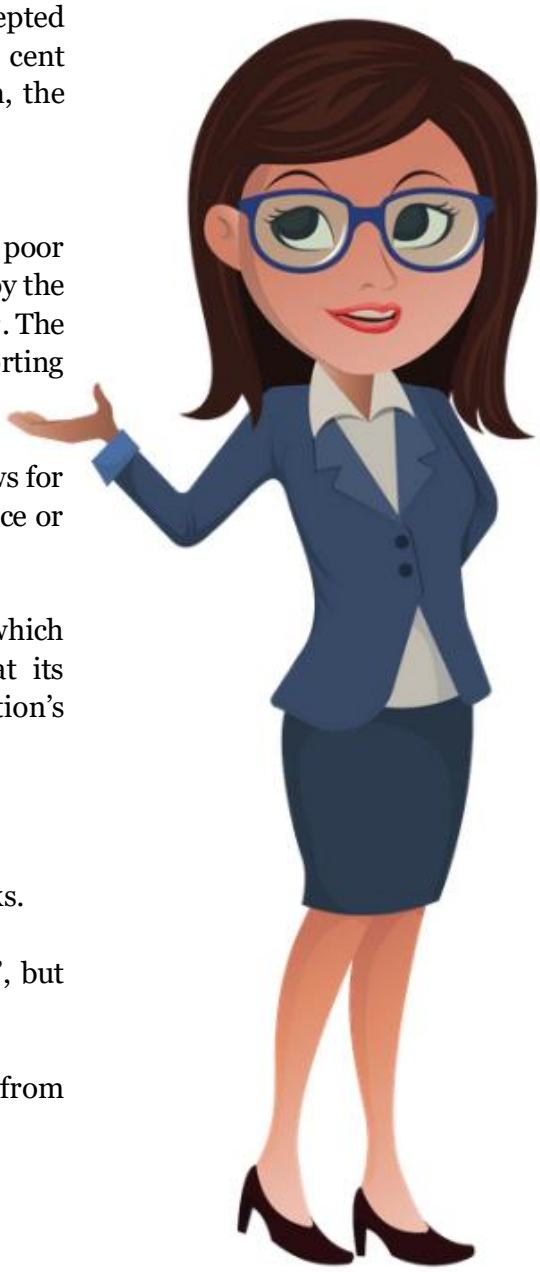
In April 2004, a shareholders' derivative complaint was filed against Riggs. The law suit alleged that eleven (11) directors breached their fiduciary duties of loyalty, honesty and care and caused a waste of corporate assets and other harms to Riggs. They failed to conduct appropriate due diligence of the bank's Middle Eastern and Equatorial Guinea customers, and failed to exercise reasonable control and supervision over Riggs and its officers and employees, in connection with Riggs' compliance with applicable banking laws. This was to be the first of several shareholder law suits brought against the bank and its management.

The OCC Fine

On 13 May 2004, Riggs was fined US$25 million by The Office of the Comptroller of the Currency (OCC) for numerous violations of the Bank Secrecy Act, relating to the Saudi Arabian and Equatorial Guinea issues, and the lack of suspicious activity reporting. This amount was the largest civil monetary penalty (at the time) ever brought against a US financial institution for violations under the Bank Secrecy Act, the statute requiring financial institutions to guard against money laundering. The OCC's report stated that the bank's internal controls "were, and continue to be, seriously deficient". "Riggs failed to properly monitor, and report suspicious transactions involving tens of millions of dollars in cash withdrawals, international drafts that were returned to the bank and numerous sequentially numbered cashiers' cheques.

Understanding the Effects - Reputational Fallout

From late 2002, until Riggs was sold to the PNC Financial Services Group in mid-2005, a series of investigations resulted in further fines and settlements which totalled US$59.0 million. Within a two (2) years' time frame, legal and consulting fees topped US$35.0 million. However, the true cost of reputational damage was clearly reflected by the drop in share price. On 15 June 2004, Riggs accepted an offer made by PNC of US$24.25 per share. On 10 February 2005, Riggs had accepted a renegotiated price of US$20 per share, indicating approximately 20.0 per cent drop in a matter of eight (8) months. Instead of achieving US$779.0 million, the shareholders accepted approximately US$643.0 million.



Lessons to be learnt

- ✓ Riggs was fined primarily because of a lack of proper internal controls, poor vigilance and inadequate procedures, which were further exacerbated by the purposeful attempt to conceal activities of great concern to the regulator. The bank's basic Know Your Customer (KYC), AML and suspicious reporting procedures were grossly inadequate.

- ✓ It is important that institutions implement adequate controls that allows for the identification of PEPs, whether that individual currently holds office or not.

- ✓ If a financial institution serves PEPs who are from jurisdictions which present a heightened level of risk, the institution must ensure that its employees are adequately trained and kept updated on the jurisdiction's risks.

- ✓ The viability of an institution is only as good as its reputation.

- ✓ Never underestimate the 'bad guys'. They can be craftier than one thinks.

- ✓ Compliance should not be seen as a department which 'costs money', but rather as a 'reputation protection department' that could save millions.

This case study was prepared by WorldCheck and extracted from https://www.world-check.com/media/d/content_whitepaper_reference/whitepaper-3.pdf.

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

@ECCBConnects

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

Eastern Caribbean Central Bank