THE FINANCIAL INTELLIGENCE UNIT-
BAHAMAS

IDENTIFIED FRAUD TRENDS & TYPOLOGIES

Presented by: **Basil Collie**, AFI, *Deputy Director*

OUR
Mission and Vision

Mission

Our vision is for The Commonwealth of The Bahamas to have a robust, dynamic and exemplary financial service industry, free from the scourge of money laundering, terrorist financing, fraud and other criminal conduct.

Vision

To proactively network with local law enforcement, regulators and international counterparts to effectively assist in detecting, assessing and eradicating all threats of money laundering and financing of terrorism to the global economy.

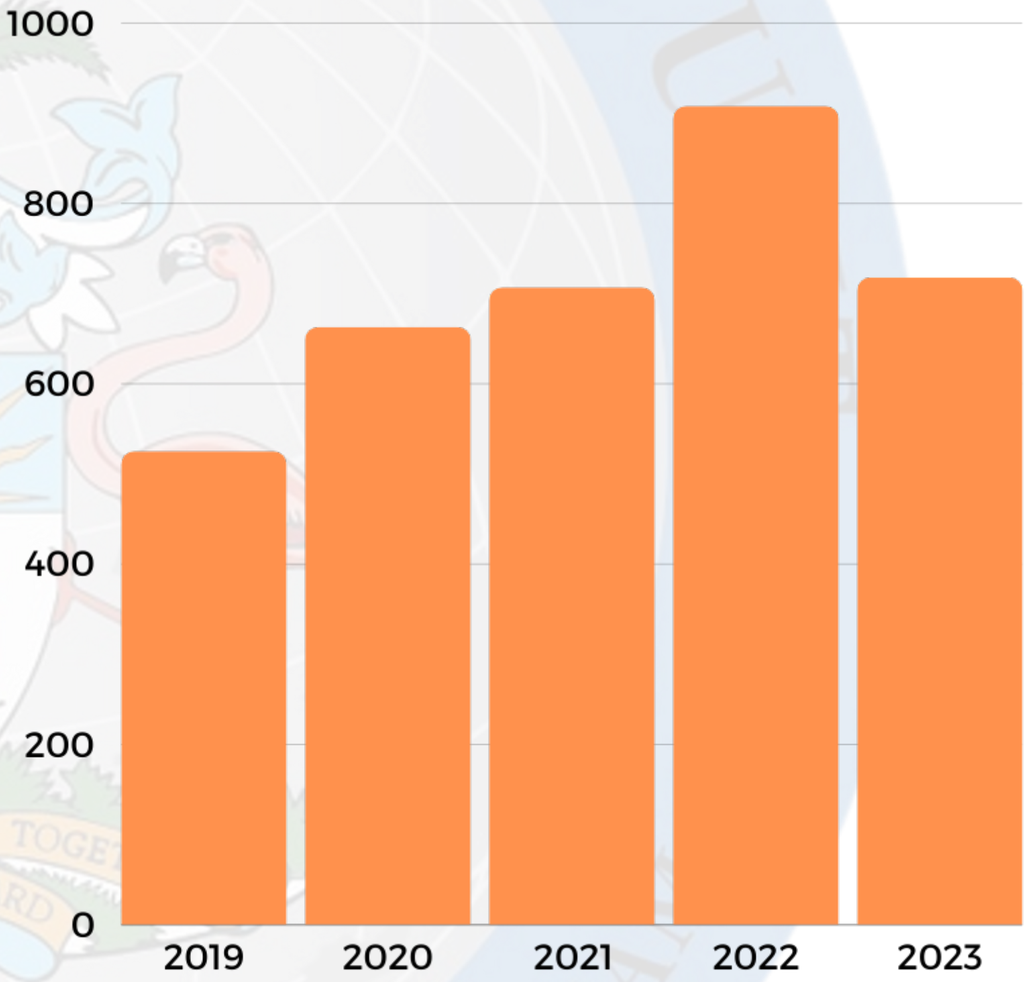
“In 2023, (IC3) received almost nine hundred thousand complaints from the American public, with potential losses exceeding $12.5 Billion dollars.”

– FBI

Investment fraud as reported by the FBI represented $4.57 Billion in 2023, while business e-mail compromise (BEC) accounted for $2.9 Billion in losses.

STRs Received
For 2019 - 2023

2019	2020	2021	2022	2023
525	663	707	908	718



STR REPORTING BY INSTITUTION TYPE

Institution Type	2023	2022	2021	2020	2019
Banks	612	342	605	573	299
Casinos	32	16	16	18	48
Trust Companies	14	57	11	25	17
Insurance Companies	4	3	11	1	3
Insurance Agent/Broker	0	2	0	0	0
Non-Bank Entities	5	338	11	0	0
Company Service Providers	2	19	9	6	9
Money Remittance Services	7	78	8	19	103
Stockbrokers	2	4	8	4	6
Law Firms	4	3	6	4	5
Regulators	0	2	5	0	5

STR REPORTING BY INSTITUTION TYPE

Institution Type	2023	2022	2021	2020	2019
Bookers/Dealers	0	0	4	4	11
Credit Unions	5	0	4	2	6
Real Estate Agents/Broker	0	0	3	0	2
Accountants	3	0	2	0	0
Securities	22	39	2	0	0
Financial Advisors	0	0	1	3	5
Investment Administrator	0	2	1	0	0
Other	0	0	0	3	1
Fund Managers	0	3	0	1	5
Gaming Establishment	1	0	0	0	0
Virtual Asset Service Provider	5	-	-	-	-

STR REPORTING BY INSTITUTION TYPE

	2023	2022	2021	2020	2019
Total Institution STR Filings	718	908	707	663	525

GROUNDS FOR DISCLOSURE/ CRIMINALITY SUSPECTED TYPES 2023

Criminality Suspected	No.
Bribery	7
Corruption	30
Counterfeit Goods	2
Cyber Crimes	3
Drugs	10
Financing Proliferation of WMD	1
Fraud	187
Illegal Gambling	2
Insider Trading	7
Not Selected	2
Other	22

GROUNDS FOR DISCLOSURE/ CRIMINALITY SUSPECTED TYPES 2023

Criminality Suspected	No.
Ponzi Schemes and Lotteries	1
Regulatory Matters	2
Tax Matters	89
Trafficking In Person	2
Unknown/Undetermined	349
UNSCR	2
Total	**718**

TRENDS IDENTIFIED

Adverse Media	Bill Stuffing	Phishing	UN Sanction Russia/Ukraine	Account Rental
Business Email Compromise	Business through Personal	Cryptocurrency Fraud	Trade Based Money Laundering	Unauthorized Fraudulent Transfers
Empty Envelope/ATM Fraud	Kiting	MTSB Transation	Professional Money Laundering	Internal Unauthorized Transfers
Online Banking Fraud	Passing Chips/Cash	Real Estate Fraud	Suspected VAT & NIB Evasion	Receipt of Unauthorized 3rd Party Transfers

Co-operation & Collaboration

SECURITIES COMMISSION OF THE BAHAMAS

CENTRAL BANK OF THE BAHAMAS

COMPLIANCE COMMISSION OF THE BAHAMAS

INSURANCE COMMISSION OF THE BAHAMAS

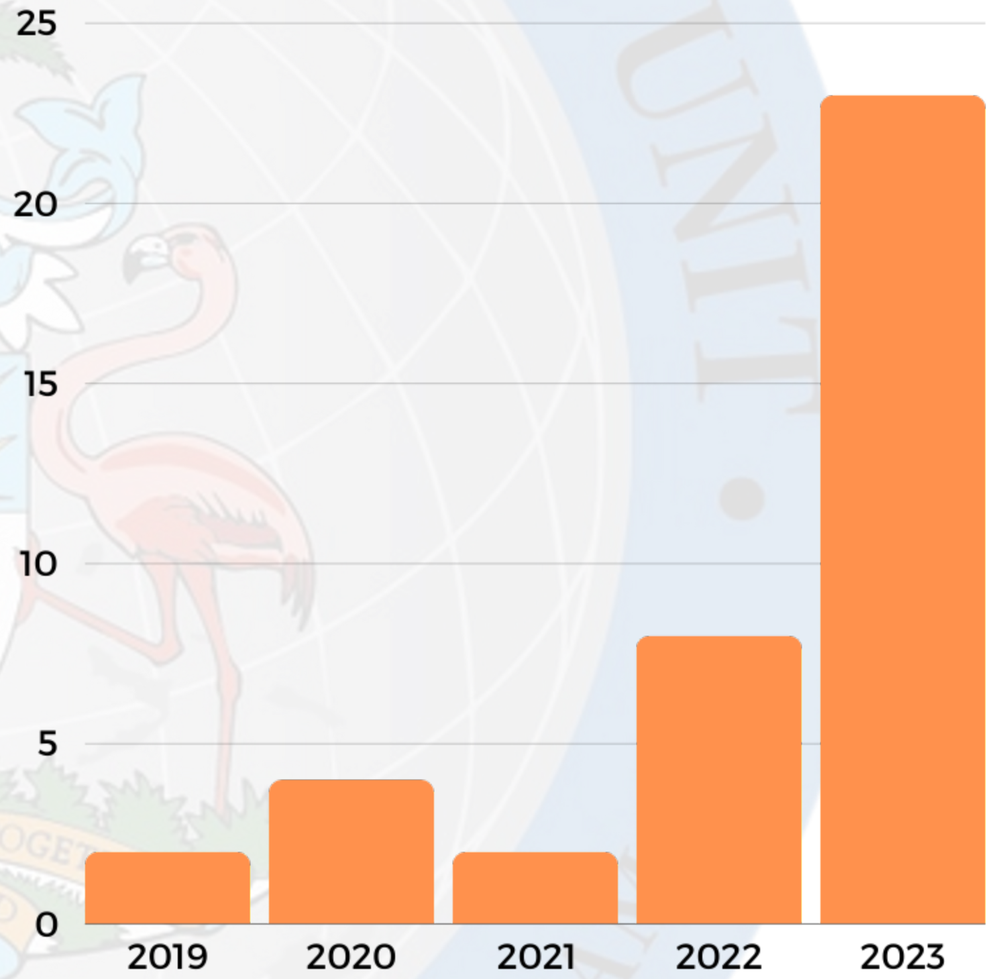
GAMING BOARD FOR THE BAHAMAS

ROYAL BAHAMAS POLICE FORCE
COURAGE INTERGRITY LOYALTY

STRs Received

Which referenced Fraudulent Cheques

2019	2020	2021	2022	2023
2	4	2	8	23



Typology #1:

Wire Fraud

Financial Intelligence Unit

(7) STR is analyzed and forwarded to the Royal Bahamas Police Force for further investigation.

Royal Bahamas Police Force

(6) STR Submitted to FIU

BAHAMIAN BANK

(1) Requests routine wire transfer to purported legitimate suppliers

Amount : BSD $600,000.00

(2) Financial institution completes seven (7) wire transfers to entities using the wire transfer details provided by client
(Unbeknownst that their Client is a Victim of a Phishing Fraud).

BSD $600,000.00

FRAUDULENT SUPPLIERS

LOCAL BAHAMIAN BUSINESS

(5) Contacted the Bank in an attempt to stop the transfer.

(3) Previous wire transfer communications via email & telephone were not from the legitimate supplier

COLD ROCK BUS1NESS SERVICES
Email:- coldrockserv1ces@gmail.com
Account Name:- Lucas Investments

TRUE-BLUE BUS1NESS SOLUTIONS
Email:- truebluebus1ness@gmail.com
Account Name:- Lucas Investments

(4) Client communicated with suppliers and learned that funds were sent to the wrong account numbers

LEGITIMATE SUPPLIERS

COLD ROCK BUSINESS SERVICES
Email:- coldrockservices@gmail.com
Account Name:- Cold Rock Business Services

TRUE-BLUE BUSINESS SOLUTIONS
Email:- truebluebusiness@gmail.com
Account Name:-True-Blue Business Solutions

Typology #2:

Wire Fraud

Financial Intelligence Unit

(9) STR is analyzed and forwarded to the Royal Bahamas Police Force for further investigation.

Royal Bahamas Police Force

(8) STR Submitted To FIU

(6)

Visited local branch of Bahamian financial institution to dispute several international wire transfers

BAHAMIAN BANK

(7)

Financial institution confirms six (6) international wire transfers completed and sent from the client's account

LOCAL BAHAMIAN BUSINESSMAN

(2) On the invitation of hacker posing as a banking official client installed remote desktop application on his pc

(3) Took Control of Client's Account

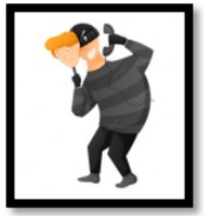
HACKER

(4) Conducted international transfers via clients online banking information acquired from pc

FOREIGN BANK

(5) Fraudulently received over $26,000.00 from Bahamian client account

(1) Previously contacted by purported bank official and led to believe he was assisting in an investigation



MARY JANE

SUSAN BLUE

Typology #3:

Cheque Fraud

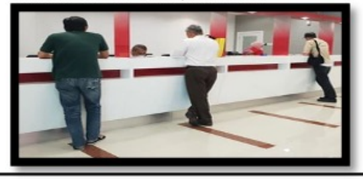
SELF-EMPLOYED MECHANIC (CLIENT)

CLIENT HELD A PERSONAL SAVINGS ACCOUNT AT FI #1
ACCOUNT BALANCE: $55.23

(1) CLIENT VISITED LOCAL BRANCH OF FI #1 AND DEPOSITED SIGNIFICANT CHEQUE DEPOSIT TOTALING $100,000.00 THROUGH ABM

(2) FI #1 PLACED HOLD ON CHEQUE

(3) CLIENT LATER VISITED FI #1 AND WAS ABLE TO ACCESS FUNDS AND WITHDREW $20,000.00.



Financial Institution #1

CHEQUE DEPOSIT PURPORTEDLY DRAWN ON ACCOUNT AT FI #2

FINANCIAL INSTITUTION #2

(4) INFORMED FI #1 THAT THE CHEQUE DEPOSIT TOTALING $100,000.00 WAS FRAUDULENT. FI #1 WAS ALSO MADE AWARE OF OTHER FRAUDELENT ACTIVITY CONDUCTED BY THE SUBJECT .

(5) FI #1 later discovered through news reports that the client and another individual were facing multiple counts of fraud and money laundering charges. The client was accused of laundering over $700,000.00

(6) STR Submitted to FIU

Financial Intelligence Unit

(7) STR is analyzed and forwarded to the Royal Bahamas Police Force for further investigation.

Royal Bahamas Police Force

FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 1 of 2023

2 August 2023

NOTICE TO ALL FINANCIAL INSTITUTIONS

The Financial Intelligence Unit (FIU) of The Bahamas hereby advises financial institutions and the public at large of incidences of fraudulent activities that are adversely affecting account holders of various commercial banks in the jurisdiction. Consequently, the public is being advised to be aware of, and take note of, the following.

The FIU has noticed an increase in Suspicious Transaction Reports (STRs) where commercial banks have reported instances of account holders reporting unauthorized online transfers to persons unrelated or unknown to them.

The FIU has identified the following information relative to these unauthorized transfers. The fraudulent activity involves two separate circumstances involving the victim and, in some cases, complicit or non-complicit recipients of the funds transferred.

Based on information received, victims reported the unauthorized transfers but would also note being contacted previously by a purported representative from the bank. The victims would then admit providing their account information to the purported representative. These individuals are victims of telephone banking fraud. Telephone banking fraud occurs when an individual is contacted by someone who is claiming to be from an organization you trust, whether it be a bank or a governmental agency. The purported representative would then advise that there is an issue with your account information or requesting verification of a recent transfer. They induce the account holder to provide them with their personal banking information. The purported representative then uses this information to either use the client's online banking or block the account holder from their account to use their online banking.

In other cases, victims have been noted to provide information as a result of an email purporting to come from their banking institution requesting that the account holder confirm their banking information to avoid being blocked from their account. The email will contain a link the account holder would click on to provide the information. This type of fraud is known as a phishing scam where the victim is induced to reveal sensitive information.

FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC NOTICE

No. 2 of 2023 15 August 2023

NOTICE TO ALL FINANCIAL INSTITUTIONS AND THE GENERAL PUBLIC

The Financial Intelligence Unit (FIU) of The Bahamas hereby advises all entities that are defined as a "Financial Institution" (FI) pursuant to Section 3 of the Financial Transactions Reporting Act, 2018, and the public at large to take note of the FIU's Public Advisory 1 of 2023 published on the FIU's website at https://www.fiubahamas.org.bs/category/advisories/ .

The FIU has noticed an increase in Suspicious Transaction Reports (STRs) where commercial banks have reported instances of account holders reporting unauthorized online transfers to persons unrelated or unknown to them.

The FIU has identified the following information relative to these unauthorized transfers. The fraudulent activity involves two separate circumstances involving the victim and, in some cases, complicit or non-complicit recipients of the funds transferred. The victim's account used for the unauthorized transfer was at some point compromised as a result of a telephone banking or phishing scam and the recipient is used as a money mule and recruited in most circumstances through a social media platform.

The FIU would like for financial institutions and the general public to guard against such fraudulent activities and would invite all persons to review the FIU's Public Advisory 1/2023 on its website for further details on these fraudulent activities, the trends identified, and precautionary measures recommended by the FIU.

The FIU appreciates your continued support and cooperation.

Mr. Emrick K. Seymour, KPM
Director
Financial Intelligence Unit
3rd Floor, Norfolk House
Frederick Street
P.O. Box SB-50086
Nassau, Bahamas
Tele: (242) 356-9808/ (242) 326-3815
Fax: (242) 322-5551
Email: director.fiu@fiubahamas.bs

Tips to Avoid Becoming a Victim of Fraud

1. If you receive a call or email and cannot verify that the same is legitimate it is advised to never provide personal account information via telephone or email and to visit your bank branch in person to confirm the veracity of the call or email.
2. It is advisable in general to be weary of any email that provides a link that requires the production of any personal information.
3. To prevent your computer system from being compromised never click on links or attachments coming from suspicious emails.
4. Hackers may use the interface of familiar websites like Amazon, Paypal, Ebay etc. If you are unsure of the information being provided it is best to leave the email and go directly to your account and check for any messages that may have been sent.
5. There are occasions where establishments would legitimately use social media platforms for recruitment. However, it has been determined that the recruitment for employment as seen in these cases is generally a part of a larger fraud scam.
6. If you are the recipient of funds that you have not legitimately earned, you are unaware of the sender or it is a transfer that you have no prior knowledge of, it is advised that this should be reported to the bank or the Royal Bahamas Police Force. Under no circumstance should the monies be withdrawn for your personal use or to remit to the fraudster.
7. For financial institutions, where such fraudulent activities are evident, the financial institution must adhere to its obligation to report these matters to the FIU as soon as practicable.
8. If you receive an email from a person purporting to be someone that you may know asking for help or money it is best to contact that person by a known telephone number. Never respond to an email message especially if you are not sure if the email is legitimate.
9. All business establishments should ensure that their IT systems are protected with security software but additionally staff should be sensitized on the dangers of phishing scams to the establishments IT infrastructure and cautioned not to download suspicious attachments or click on suspicious links.
10. As a rule, one should check online accounts on a regular basis to ensure the activity on the account is in keeping with known activity conducted by you.
11. As a general rule it is advisable to NEVER give out personal information via telephone or online.
12. Although not a conclusive sign but in general most fraudulent emails may contain spelling and grammatical errors.
13. Persons should also be wary of purchasing items from places that post advertisements on social media but rarely have any other online footprint.

The Financial Intelligence Unit – The Bahamas
MLRO Forum

""A chain is only as strong as its weakest link..."

Thank You

For Your Attention

Visit Our Website
www.fiubahamas.org.bs