FINANCIAL INVESTIGATIONS DIVISION

FINANCIAL INTELLIGENCE UNIT

Virtual Assets Typology Report

(Suspicious Reports 2022 - 2024)

FID-TR-2026-02

Table of Contents

OVERVIEW 2

METHODOLOGY 2

Report Statistics 3

Monetary Value of STRs Submitted 4

Analysis of Suspicious Reports 5

Primary Indicators Selected 5

Analysis of Reports Reasons for Suspicion 6

Use of Financial Intelligence 8

Profile of Subjects Reported 9

Parish/Location 9

Occupation & Age 10

Conclusion 11

INFORMATION PURPOSES ONLY

Typologies Identified from STRs relating to Virtual Assets (Jan 2022 – Dec 2024)

OVERVIEW

The Financial Services Commission (FSC) having completed its first risk assessment of the Virtual Assets Service Provider (VASP) Sector in 2023, is subsequently revising same to reflect the sector's current risk profile. In order to ensure that all available information is captured in the risk assessment the FSC requested the following information from the Financial Investigations Division (FID) for a two (2) year period 2022 to 2024:

i) the number of STRs received that were VA-related;

ii) the underlying criminal activities related to the number of STRs received;

iii) details regarding whether any of the STRs were converted to case disclosures for further investigations; and

iv) an indication as to whether the FID requested or received requests in relation to VASPs linked activities from other jurisdictions or any international agency.

This report seeks to provide the relevant statistics, nature of transactions and the activities identified by the reporting entities that were deemed to be related to virtual assets during the period January 2022 to December 2024. All dollar values provided are reflected in Jamaican dollars (J$), unless otherwise stated.

METHODOLOGY

Currently, the national framework and infrastructure for a VASP sector is not fully developed and therefore, there are no direct reporting requirements from the sector.

The FID is, however, aware that the digital environment has allowed Jamaicans the opportunity to participate in the virtual asset market. The goAML database was interrogated to ascertain the information required with the following search criteria:

Search Field	Identifiers	Alternative Identifiers	Digital Asset Platforms (Cryptocurrency Merchants) identified
Reason for Suspicion	• Crypto • Bitcoin	• Crypto currency • Cryptocurrency • Cryptocurrency Miner • Digital Assets • Bitcoin • Forex Trading - Bitcon • USDT • Ethereum coins • NFTs	• CEX.IO • Deriv.com • Mercuryo/ Mercuryo Vilnius • FPMarkets • Telegram • Kaizen Data • Etana Custody Inc. • Kryptovest Investment Forum • Metatrader5 (MT5) • C Trader • WM Cryptic Consultant Limited • Coinmama • IC Markets

INFORMATION PURPOSES ONLY

Typologies Identified from STRs relating to Virtual Assets (Jan 2022 – Dec 2024)

Search Field	Identifiers	Alternative Identifiers	Digital Asset Platforms (Cryptocurrency Merchants) identified
			• Instacoins • Bitcoin Investment • FX Scalper • Banxa/ Banxa Changel • hfm.com • xnglobal.com • Payward Trading Limited • Key Vision Development Limited • FX Scalper X • switchere.com • MT4 Apps • Blockfi Trading LLC • Interactive Brokers LLC • Paxful • Kracken.com • Capital.com • Alchemy GPS Europe

Report Statistics

For the period, January 2022 to December 2024, ninety-five (95) reports were received from financial institutions that included Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs) and Authorized Disclosure (Request for Consent) Reports (ADRs). The sectors that reported were the Commercial Bank and the Remittance sectors. Five (5) of the eight (8) commercial banks and two (2) of the ten (10) remittance agencies contributed to the statistics for the period under review:

Sectors	2022		2023			2024			Grand Total
	STR	SAR	STR	ADR	SAR	STR	ADR	SAR	
BANK (Commercial)	16	0	12	3	0	35	2	1	69
Remittance	6	1	15	0	1	2	0	1	26
Grand Total	**22**	**1**	**27**	**3**	**1**	**37**	**2**	**2**	**95**

INFORMATION PURPOSES ONLY

Monetary Value of STRs Submitted

The eighty-six (86) STRs submitted for the period under review consisted of five hundred and sixty-three (563) transactions with a total monetary value of approximately J$208M (or equivalent US$32,702[1]). The transactions reported were mainly electronic namely:

- Account to Account
- Account to Cryptocurrency Merchant and vice versa
- VISA Direct to Account

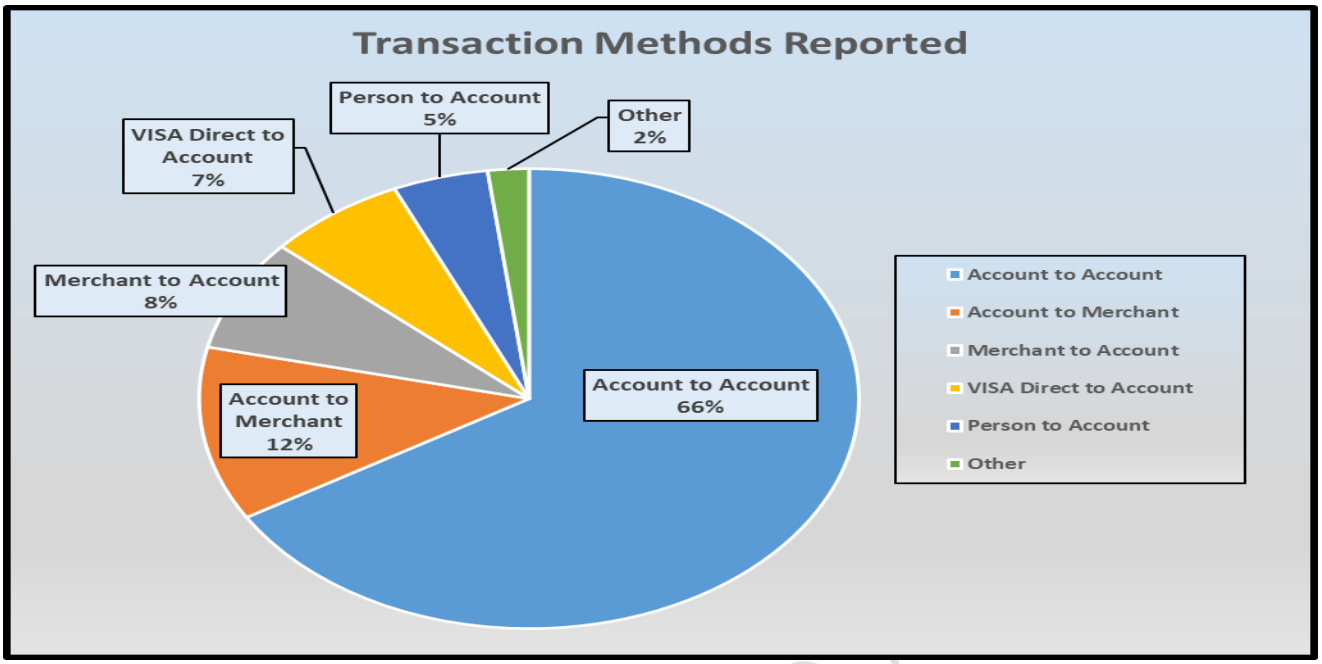
Electronic transactions accounted for 93% (J$194M/US$30,501) of the total monetary value of J$208M, while 7% (J$14M/US$2,201) involved cash deposits. See summary in the table and chart below;

Agency Business Type	2022			2023			2024			Total Report Count	Total Tran. Count	Total Tran. Amount J$
	Report Count	Tran. Count	Tran. Amount J$	Report Count	Tran. Count	Tran. Amount J$	Report Count	Tran. Count	Tran. Amount J$			
Commercial Bank	16	170	79,279,969.01	12	123	47,939,437.84	35	235	78,840,096.89	63	528	206,059,503.74
Remittance	6	6	587,047.13	15	24	1,356,907.44	2	5	128,529.78	23	35	2,072,484.35
Grand Total	**22**	**176**	**79,867,016.14**	**27**	**147**	**49,296,345.28**	**37**	**240**	**78,968,626.67**	**86**	**563**	**208,131,988.09**

It should be noted that SARs (4) and ADRs (5) are classified as activity-based reports and do not involve a dollar value, hence the table above only represents the dollar value of STRs (86) reported.

[1] BOJ US Weighted Average Rate Selling – US$157.22

INFORMATION FOR PURPOSES ONLY

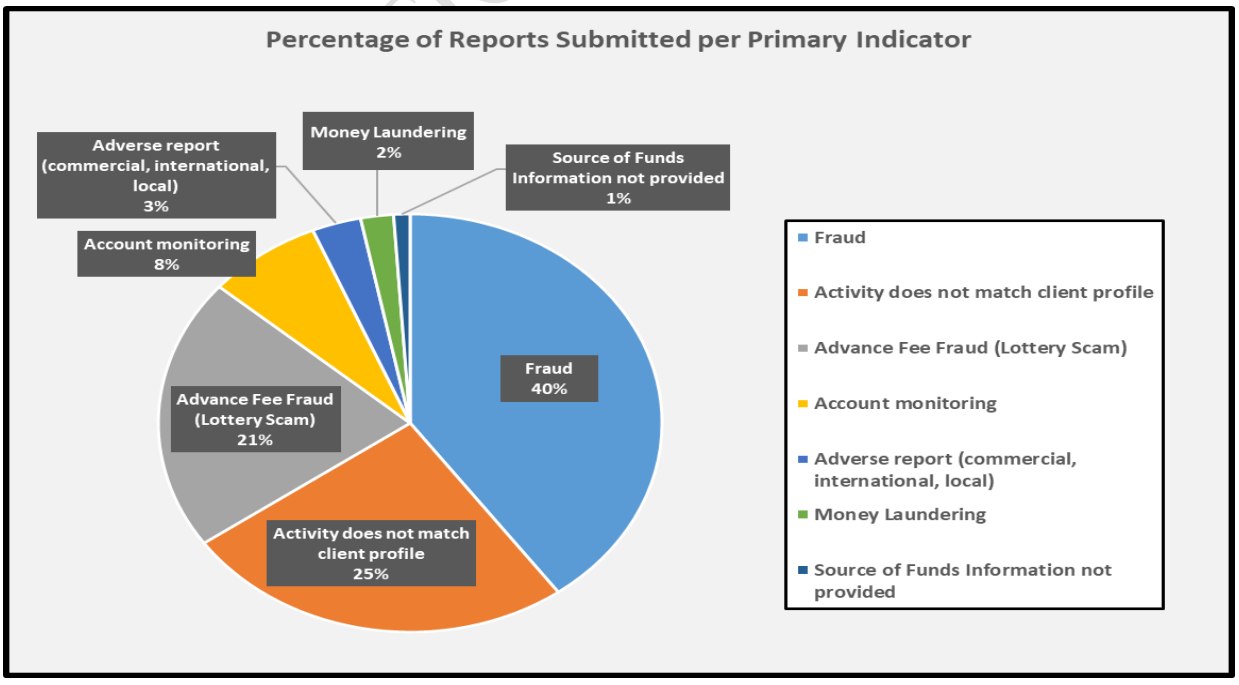


Analysis of Suspicious Reports

Primary Indicators Selected

The primary indicators selected by the reporting entities were **Fraud, Activity does not match client profile** and **Advance Fee Fraud. Advance Fee Fraud** is most reported by the remittance sector with the activities related to multiple senders to a receiver and/ or mutual sender to multiple recipients from overseas jurisdictions.

See below the percentage of reports that were submitted for the indicators specified by the reporting sector for the period under review:



Typologies Identified from STRs relating to Virtual Assets (Jan 2022 – Dec 2024)

The total monetary value of each indicator selected and the number of transactions involved for the STRs are detailed below:

Main Indicator	Report Count	Total Tran.	Total Tran. Amount J$
Activity does not match client profile	24	258	131,136,755.53
Account monitoring	7	70	49,880,857.28
Fraud	38	158	13,148,992.28
Adverse report (commercial, international, local)	3	13	6,212,304.00
Money Laundering	2	25	3,729,584.90
Source of Funds Information not provided	1	10	2,562,915.76
Advance Fee Fraud (Lottery Scam)	20	29	1,460,578.34
Grand Total	**95**	**563**	**208,131,988.09**

Analysis of Reports Reasons for Suspicion

Further analysis of the reasons for suspicion provided by the entities, the FIU extracted the following details:

Suspicion Concluded	Summary of activities highlighted in the reason by Reporting Entities:	Report Count	Tran. Count	Total Tran. Amount J$
Activity does not match client (involving cryptocurrency)	1. Increase ABM cash deposits but depletion via POS transactions on cryptocurrency trading platforms *(CEX.IO, Coinmama, IC Markets, Instacoins, FX Scalper)* 2. VISA direct inflows with source being from FX online trading done on *MT4 Apps* and income generated sent to cryptocurrency trading platforms (*Any Exchange*, *CEX.IO, Payward Trading Limited)* 3. Incoming transfer representing profits earned overtime that were then converted from cryptocurrency to USD through a broker company *(Etana Custody Inc.)* 4. Increase in third party deposit activities to client account that were mainly depleted via increase transactions through a cryptocurrency trading platform *(FPMarkets, Interactive Brokers)* and a loan crypto entity that offers loans to crypto asset owners who collateralize the loan with their crypto assets *(Blockfi Trading LLC).* Account being used for trading cryptocurrencies on behalf of third parties. 5. Account rental scam to receive third party transfers to client account that is then depleted via transfers to *PayPal* account and third party at another financial institution for conversion into cryptocurrency	25	287	178,431,709.80

INFORMATION PURPOSES ONLY

Typologies Identified from STRs relating to Virtual Assets (Jan 2022 – Dec 2024)

Suspicion Concluded	Summary of activities highlighted in the reason by Reporting Entities:	Report Count	Tran. Count	Total Tran. Amount J$
Crypto Currency Trading (Warner Media)	✓ Fraudster accounts receive third party transfers representing USDT exchange of cryptocurrency for an online employment scam referred to as: ➢ ***Warner Media Ponzi Scheme***. ➢ ***Online Video Liking Scam*** ➢ ***Online Employment Scam*** This scheme, recruiters (victims) had to make an investment and receive monthly returns in the form of USDT cryptocurrency by completing virtual tasks. The cryptocurrency trading platform used was *CEX.IO, Deriv.com and Telegram*	14	110	16,877,915.61
Social Media Fraud (Crypto currency Investment)	✓ Fraudster account receives transfer to account representing an investment based social media advertisement (Instagram, Facebook) regarding trading and ability to get high returns. Victim also was provided with: 1. a website link in the name of *Kryptovest Investment Forum; tradingstarten.com* providing opportunity to converse with "investors"; and 2. additional instructions to make additional deposits representing "synchronizing/extraction fee. One (1) of the methods of depletion of the fraudulently obtained funds was POS transactions to crypto currency trading platform merchants - *CEX.IO & Mercuryo*. ✓ Electronic transfer to fraudster account based on instructions provided to further credit to the victims cryptocurrency account. The funds were instead transferred to a third party at another institution along with several POS transactions for online gaming. ✓ Advance Fee Fraud (Lottery Scamming) via: Overseas sender responding to investment opportunity with crypto currency and bitcoin from a social media advertisement (Instagram) ➢ Overseas sender contacted by fraudster who stated he/ she is a representative of *XNGLOBAL.COM Investment Company* and that funds sent would be invested in cryptocurrency ➢ Overseas sender contacted by fraudster who invited the sender to make an investment	40	93	4,683,808.44

INFORMATION PURPOSES ONLY

Typologies Identified from STRs relating to Virtual Assets (Jan 2022 – Dec 2024)

Suspicion Concluded	Summary of activities highlighted in the reason by Reporting Entities:	Report Count	Tran. Count	Total Tran. Amount J$
	into stocks, trade and cryptocurrency and was guaranteed greater returns on his investments			
Unauthorized third party transfer (involving cryptocurrency trading)	✓ Fraudster account receives several unauthorized third party transfers with one (1) of the methods of depletion noted to be POS transactions to crypto currency trading platform merchants - *CEX.IO, Mercuryo Vilnius, Paxful Platform* ✓ Fraudster account receives unauthorized third party transfer with client indicating the transfer was for crypto currency sold to the victim and that the account is used for trading crypto currency	16	73	8,138,554.24
Grand Total		**95**	**563**	**208,131,988.09**

Use of Financial Intelligence

From the reports submitted, seventeen (17) were used to develop five (5) intelligence reports that captured nine (9) of the subjects with a total transaction value of J$58M. These intelligence reports were all submitted by the commercial banks and were disseminated to the Financial Crimes Investigations Branch of the division for further investigations to be undertaken. The preliminary offences identified from the analysis were:

- Fraud - Online Employment Scam/ Pyramid Scheme
- Lottery Scamming
- Money Laundering *(e.g. illegally obtained proceeds converted to virtual assets and reconverted to acquire real property etc.)*

INFORMATION PURPOSES ONLY

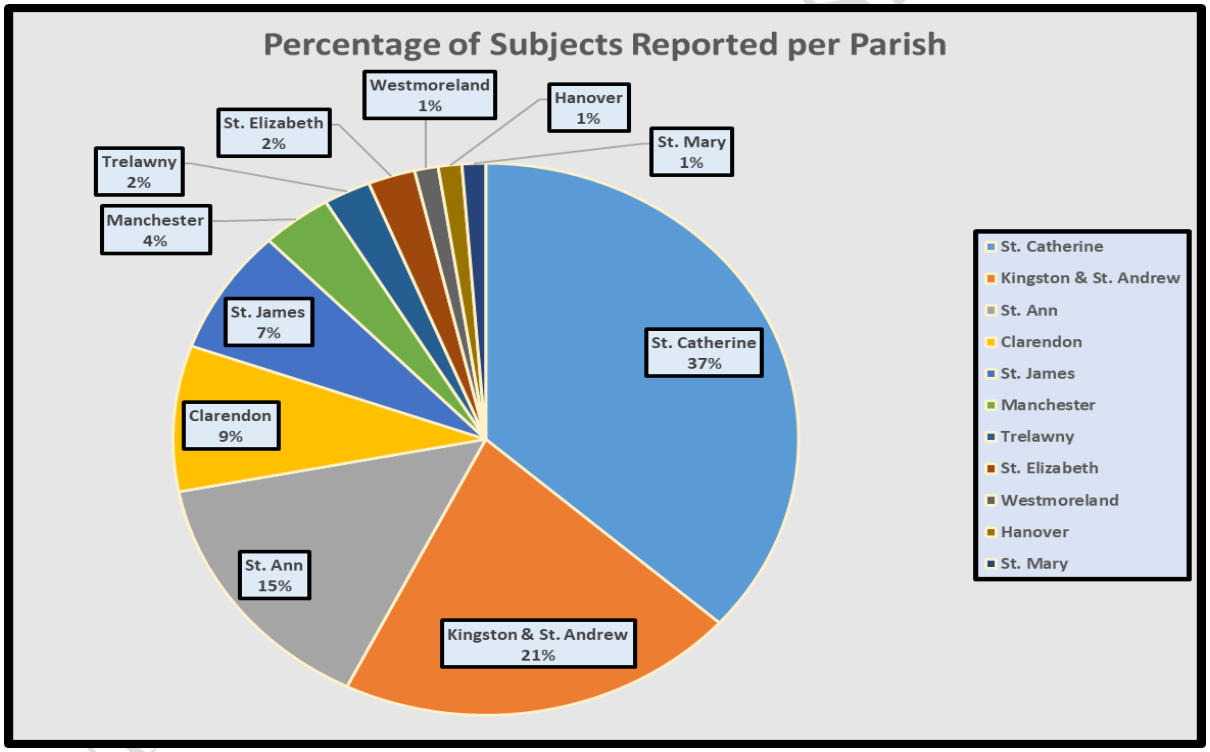
Profile of Subjects Reported

Ninety-five (95) reports were submitted for the period January 2022 to December 2024 and captured eighty-two (82) subjects/ customers. The majority were Jamaican nationals, at least 98% (80) individuals; with two (2) noted to be Jamaican residents with Dominican Republic and St. Vincent and the Grenadines nationalities. The most frequently used addresses were linked to the parishes of St. Catherine, Kingston & St. Andrew and St. Ann.

Additionally, the subjects mainly worked in the Support Services as Customer Service Representatives and Collection Agents within the age groups of 20-39. See details below:

Parish/Location

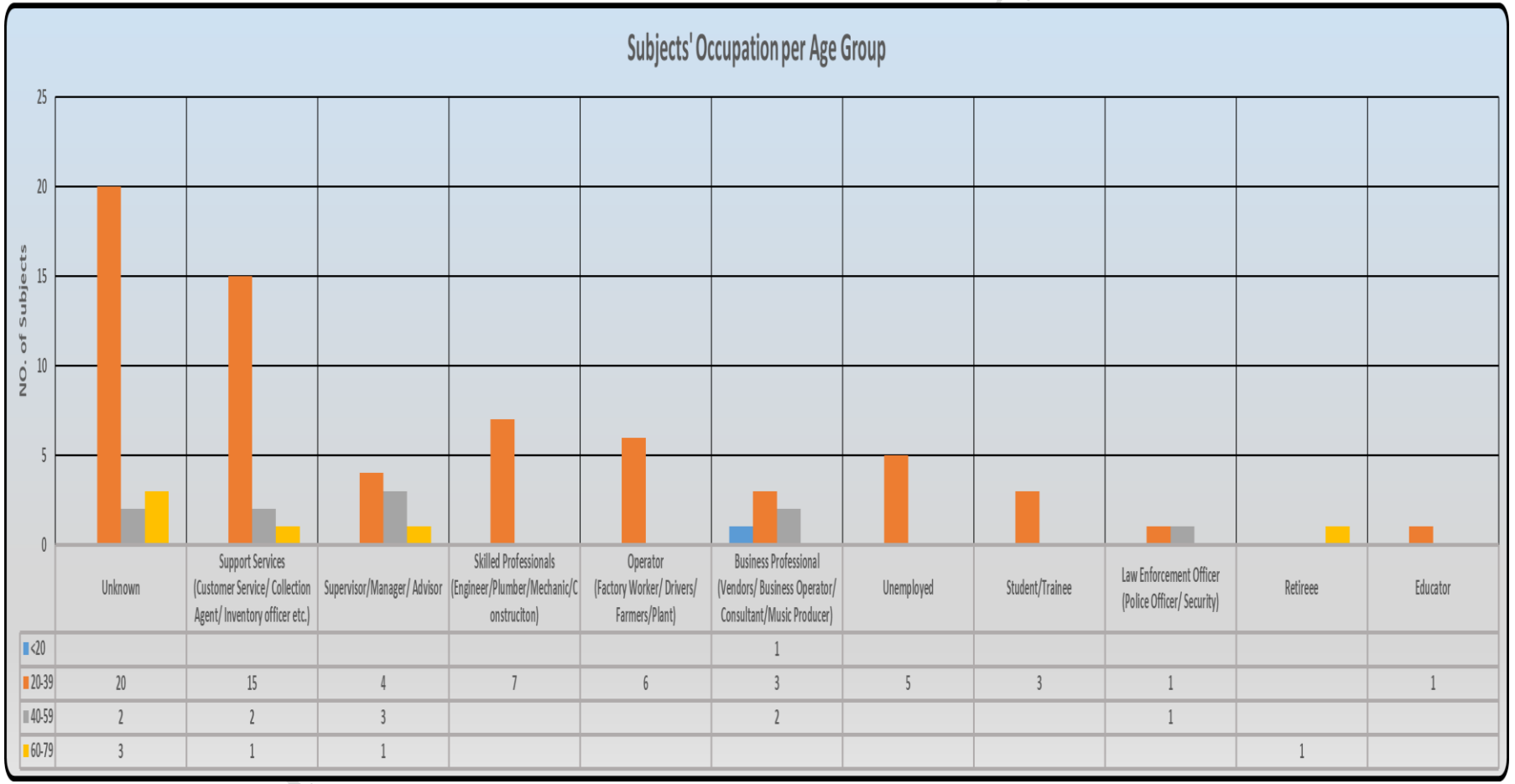
St. Catherine accounted for approximately 37% of the total number of subjects reported, that is thirty (30) subjects. Noting that a large number of the Business Processing Outsourcing (BPO) sector is located in St. Catherine. See chart below:



INTERNAL USE ONLY

Occupation & Age

From the reports submitted, 70% (57 subjects) of the subjects' occupations were specified with 32% of that total representing subjects who were in the support services field, inclusive of customer service representatives and collection agents who were within the 20 – 39 age group. Overall, the 20-39 age group accounted for approximately 79% (65 subjects) of the total number of subjects reported (82) subjects, for the period under review. See graph below the different occupations captured per age group for the reports submitted:



	Unknown	Support Services (Customer Service/ Collection Agent/ Inventory officer etc.)	Supervisor/Manager/ Advisor	Skilled Professionals (Engineer/Plumber/Mechanic/Construciton)	Operator (Factory Worker/ Drivers/ Farmers/Plant)	Business Professional (Vendors/ Business Operator/ Consultant/Music Producer)	Unemployed	Student/Trainee	Law Enforcement Officer (Police Officer/ Security)	Retireee	Educator
<20						1					
20-39	20	15	4	7	6	3	5	3	1		1
40-59	2	2	3			2			1		
60-79	3	1	1							1	

Conclusion

Advancements in technology have expanded the range of online banking services offered by financial institutions, enabling customers to conduct an increasing number of transactions without face-to-face interaction. Conversely, the growing interconnectedness of financial systems has also heightened institutions' exposure to fraud, making it a key inherent risk and vulnerability associated with the delivery of these services.

The activities reported by the financial sector involved more cyber related fraud methods that mainly included:

- Unauthorized transfer/ access to client's accounts; and
- Consumer fraud with social media platforms to advertise consumer products, investment and online employment opportunities in exchange for something, which is never honoured. Hence "obtaining money through false pretence".

The funds that are fraudulently obtained are now being depleted through transactional activities with virtual asset platforms that trades/ sells cryptocurrency. Additionally, the financial sector reported clients whose activities were not in line with their profile as there were increase electronic transfers to their accounts from virtual asset platforms. These clients indicated that they are either cryptocurrency miners and/ or traders and the inflows are the profits made. However, based on their profile in terms of age and occupation, the source of their initial investment for the volume and value of returns are questionable.

Information reported by financial institutions indicates that the increased digitalisation and interconnectedness of the financial system, particularly through online banking and electronic payment services, have heightened exposure to cyber-enabled fraud. The principal vulnerabilities identified include;

- unauthorised access to customers' accounts;
- the fraudulent transfer of funds; and
- consumer scams facilitated through social media platforms. These scams commonly involve the promotion of fictitious consumer products, investment opportunities, and online employment offers in exchange for payment, goods, or other consideration that is never delivered.

Such activities may constitute obtaining money by false pretences and generate proceeds that may subsequently be transferred through the financial system.

Of particular relevance to the assessment of virtual asset-related risks is the reported use of cryptocurrency trading platforms and other virtual asset services to move or dissipate funds obtained through fraudulent activities. Financial institutions have also identified customers whose transaction patterns appear inconsistent with their established customer profiles, including increased electronic transfers into their accounts originating from virtual asset platforms. Some customers have attributed these inflows to profits earned from cryptocurrency mining or trading. However, inconsistencies between the customers' stated occupations, ages, apparent financial circumstances, and the volume and value of the reported returns raise

INFORMATION PURPOSES ONLY

questions regarding the legitimacy of the underlying investments and the source of the initial capital used to generate those returns.

These indicators suggest potential vulnerabilities at the intersection of cyber-enabled fraud, the traditional financial system, and virtual asset transactions. While the reported activity does not, in itself, establish that the funds are illicit or that the customers are engaged in money laundering, it highlights the need for further examination of the source of funds, the origin of initial investments, the nature of virtual asset transactions, and the extent to which VASPs may be used to receive, transfer, convert, or conceal proceeds of crime.

Accordingly, the assessment of Jamaica's VASP risk profile should consider the extent to which virtual asset services may be exploited to facilitate the movement and conversion of fraud proceeds, the vulnerabilities arising from transactions between financial institutions and VASPs, and the adequacy of existing customer due diligence, transaction monitoring, suspicious transaction reporting, and other AML/CFT/CPF controls. The findings would support a more comprehensive understanding of the sector's inherent risks and inform the prioritisation of regulatory and supervisory measures under Jamaica's developing VASP framework, consistent with the risk-based approach promoted by FATF Recommendation 15.

INFORMATION PURPOSES ONLY