



TYPOLGY REPORT: CRYPTOCURRENCY

FASU Reference: TYP/004/2023
Issued Date: September 2023

Disclaimer

This report is intended for the *Financial Institutions* **ONLY** for informational purposes and should under no circumstances be disclosed to any third party. Any person who internationally or recklessly discloses this information will be subject to fines under Section 95 of the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (AML/CTF Act).

Legal Mandate

The Financial Analysis and Supervision Unit (FASU) publishes this typology in accordance with Section 72(2)(b) of the AML/CTF Act.

DOCUMENT CONTROL

Version Control

Version	Date Issued	Document Status	Document Author
1	29 Sept 2023	Draft	FASU IMD
2			
3			
4			

CRYPTOCURRENCY

Definition of Terms

Blockchain – is a digital ledger of transactions that are distributed across the entire network of computers (or nodes) on the blockchain. Distributed ledgers use independent nodes to record, share, and synchronize transactions in their respective electronic ledgers instead of keeping them in one centralized server. (Merriam-Webster, 2023)

Cryptography - is the method of securing important data from unauthorized access. In the blockchain, cryptographic techniques are a part of security protocols. It secures a transaction taking place between two nodes in a blockchain network. (Data-Flair, 2023)

Distributed Ledger - A distributed ledger is a database that is spread across various computers, nodes, institutions, or countries accessible by multiple people around the globe. (wvaibhava, 2023)

WHAT IS IT?

Cryptocurrency is a digital currency that uses cryptography for security and operates on decentralized technology known as blockchain. Unlike traditional currencies issued by governments (also known as fiat currencies), the value of cryptocurrencies are typically not controlled by any central authority, such as a central bank or government. Instead, they rely on a distributed ledger technology to record transactions and maintain the integrity of the currency.

Cryptocurrency enables anyone anywhere to send and receive payments virtually without going through the traditional banking system. The first and most popular cryptocurrency is Bitcoin and it was created in 2009. Since then, thousands of other cryptocurrency have been created. Each with its own unique features and vision for their utility. The legality of cryptocurrency varies from one jurisdiction to another.

Terrorist groups, tax evaders and transitional crime groups have been using cryptocurrency to finance their activities and evading tax around the world, because of anonymity. Terrorist groups, criminal groups and tax evaders are developing their own cryptocurrency trading platform (Cryptocurrency Brokers) and are targeting countries without regulatory oversight to convert fiat currency to cryptocurrency.

In Papua New Guinea cryptocurrency is not regulated by the Bank of Papua New Guinea (Central Bank) through its Prudential as well as Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) regulation and supervision; or any other authorities¹. Countries like PNG that do not have a regulatory oversight will be difficult to trace a transaction hence may be targeted by criminals using cryptocurrencies or virtual assets to launder illicit proceeds and fund terrorist activities. In 2017, Papua New Guinea conducted its National Risk Assessment (NRA) on the threats and vulnerabilities of money laundering (ML) and terrorist financing (TF) and identified that TF was low risk.

¹ <https://www.bankpng.gov.pg/news-events/cryptocurrencies-and-blockchain-technology/>

However,

To Robert Haus,
Douglas St & Cuthbertson St
P.O Box 121, Port Moresby,
National Capital District,
Papua New Guinea
Telephone: (+675) 322 7149,
Fax: (+675) 321 1617
Website: www.bankpng.gov.pg

29 September 2023

Mr. Mark Robinson
Group Chief Executive Officer
Bank South Pacific Financial Group Limited
PO Box 78
Port Moresby
National Capital District

Dear Mr. Robinson,

TYPOLGY REPORTS

As part of the Financial Analysis and Supervision Unit's (FASU) mandated functions under the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (the Act), section 72(2)(b) includes among those functions the development of typology reports to raise awareness of money laundering and obligations on Financial Institutions (FIs) and Designated Non-financial Business and Professions (DNFBP) under the Act.

FASU hereby shares the following typology reports on:

- Government Fraud
- Motor Vehicle Dealers
- Cryptocurrency
- Money Laundering Using Visa Debit Cards

The production of these typology reports is based on the recently analyzed reported suspicious matter reports (SMR).

The development of these typology reports is an effort to inform the financial institutions of the emerging trends in financially motivated crimes and apply effective controls and mitigation measures.

This report is intended for the *Financial Institutions* **ONLY** for informational purposes and should under no circumstances be disclosed to any third party. Any person who internationally or recklessly discloses this information will be subject to fines under Section 95 of the AML/CTF Act.



**BANK OF PAPUA NEW GUINEA
FINANCIAL ANALYSIS AND SUPERVISION UNIT**

INTER-OFFICE MEMORANDUM

TO: Mr. Emete Enare
Manager – Policy Development and Coordination Division (PDCD)
Financial Analysis and Supervision Unit (FASU)

FROM: Mr. Edric Ogomeni
Manager – Intelligence Management Division (IMD)
Financial Analysis and Supervision Unit (FASU)

SUBJECT: INTERNAL DISSMEMINATION OF TYPOLOGY REPORTS

REF:

Action Officer: [SA6037](#)
Senior Review:

DATE: 29 September 2023

Background

As part of the Financial Analysis and Supervision Unit's (FASU) mandated functions under the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (the Act), section 72(2)(b) includes among those functions the development of typology reports to raise awareness of money laundering and obligations on Financial Institutions (FIs) and Designated Non-financial Business and Professions (DNFBP) under the Act.

The Intelligence Management Division (IMD) hereby shares its typology reports on

- Government Fraud
- Motor Vehicle Dealers
- Cryptocurrency
- Money Laundering Using Visa Debit Cards

Recommendation

I recommend that you consider the information provided for your team's supervisory oversight.

.....

Attach:

1 Typology Report on:

- Government Fraud
- Motor Vehicle Dealers



**BANK OF PAPUA NEW GUINEA
FINANCIAL ANALYSIS AND SUPERVISION UNIT**

INTER-OFFICE MEMORANDUM

TO: Mrs. Rosa Banik
Manager – Supervision and Compliance Division (SCD)
Financial Analysis and Supervision Unit (FASU)

FROM: Mr. Edric Ogomeni
Manager – Intelligence Management Division (IMD)
Financial Analysis and Supervision Unit (FASU)

SUBJECT: **INTERNAL DISSMEMINATION OF TYPOLOGY REPORTS**

REF:

Action Officer: [SA6037](#)
Senior Review:

DATE: 29 September 2023

Background

As part of the Financial Analysis and Supervision Unit's (FASU) mandated functions under the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (the Act), section 72(2)(b) includes among those functions the development of typology reports to raise awareness of money laundering and obligations on Financial Institutions (FIs) and Designated Non-financial Business and Professions (DNFBP) under the Act.

The Intelligence Management Division (IMD) hereby shares its typology reports on

- Government Fraud
- Motor Vehicle Dealers
- Cryptocurrency
- Money Laundering Using Visa Debit Cards

Recommendation

I recommend that you consider the information provided for your team's supervisory oversight.

.....

Attach:

1 Typology Report on:

- Government Fraud
- Motor Vehicle Dealers
- Cryptocurrency



BANK OF PAPUA NEW GUINEA
FINANCIAL ANALYSIS AND SUPERVISION UNIT

INTER-OFFICE MEMORANDUM

TO: Mr. Wilson Onea
Acting Director
Financial Analysis and Supervision Unit (FASU)

FROM: Mr. Edric Ogomeni
Manager - Intelligence Management Division (IMD)
Financial Analysis and Supervision Unit (FASU)

SUBJECT: SEEKING APPROVAL FOR THE ISSUANCE OF THE TYPOLOGY REPORTS

REF:

ACTION OFFICER: A6037

REVIEW:

DATE: 29 September 2023

Recommendation

I recommend that you:

- Approve the issuance of the typology reports to the commercial banks; and
- Sign the attached cover letters to the commercial banks.

Background

Section 72(2)(b) of the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (the Act) requires the Financial Analysis and Supervision Unit (FASU) to develop typology reports to raise awareness of money laundering and obligations on Financial Institutions (FIs) and Designated Non-financial Business and Professions (DNFBP) under the Act.

FASU has developed the following typology reports on:

- Government Fraud
- Motor Vehicle Dealers
- Cryptocurrency
- Money Laundering Using Visa Debit Cards

The production of these typology reports is based on the recently analyzed reported suspicious matter reports (SMR).

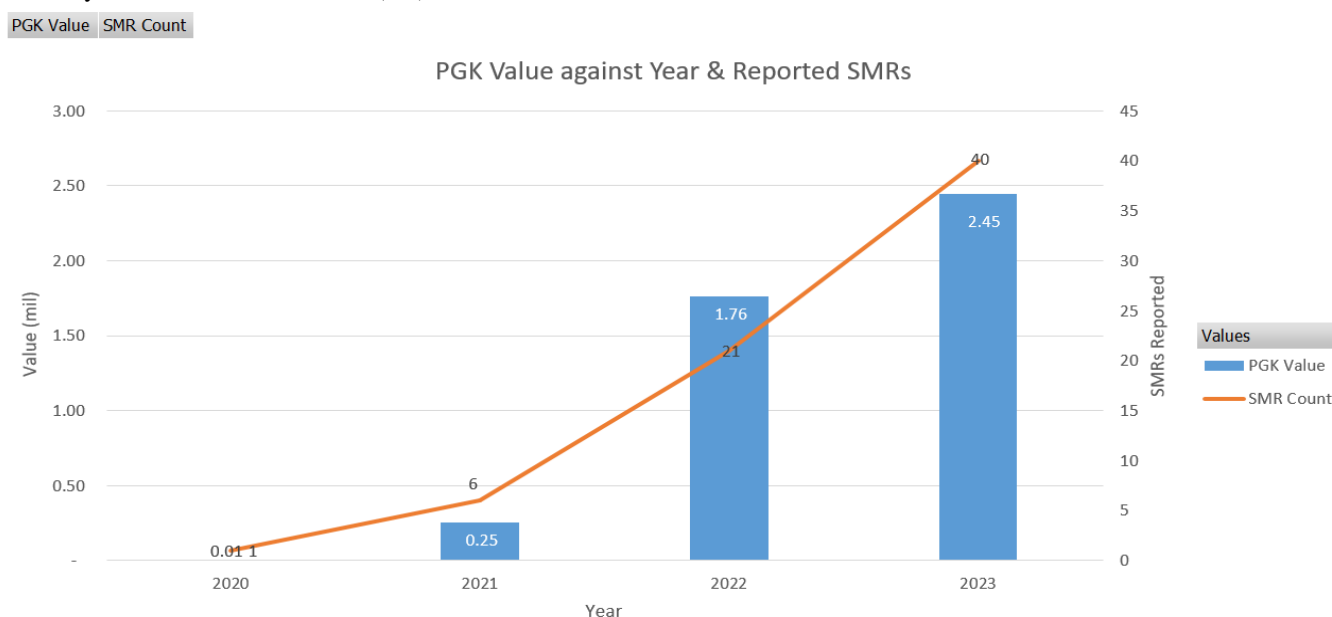
Government Fraud	Misuse and abuse of public funds still remains as one of the top five money laundering risks in PNG. Over K1 billion was reported to FASU as suspicious matter reports between August 2018 – August 2023.
-------------------------	---

Cryptocurrency Purchase Process

Cryptocurrency purchasing online using Visa cards involves a straightforward process that involves little to no KYC at all (Khlebnikova, 2023). Some of these exchanges have a limit to the amount of crypto you can withdraw, on the other hand, there are some that have no restrictions on how much you can withdraw at one time.

SMRs

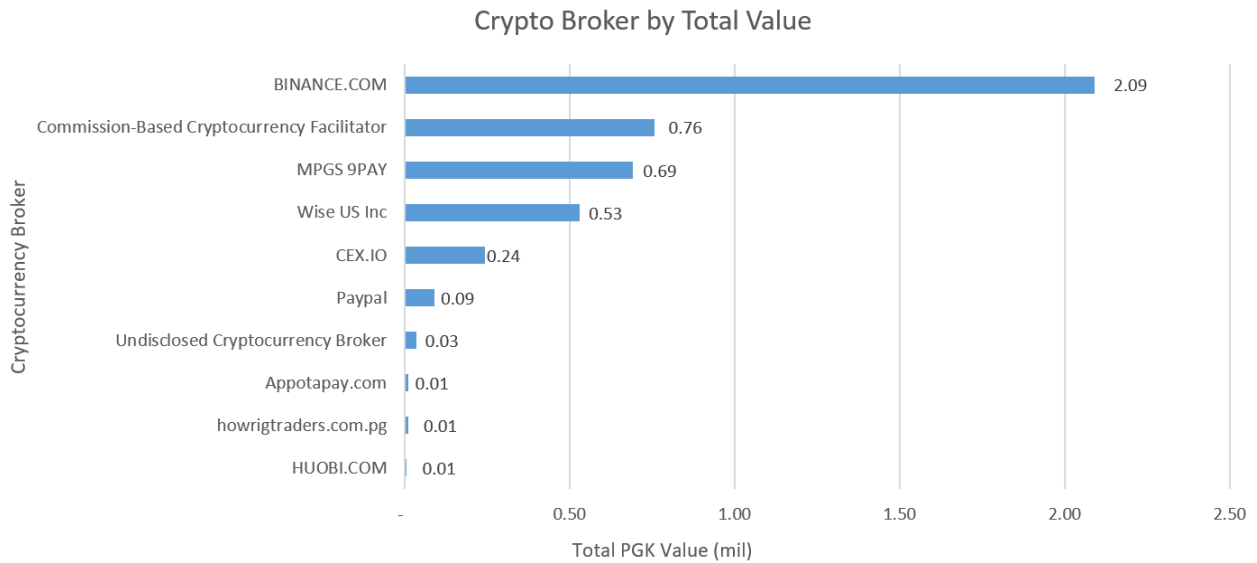
Between January 2020 and August 2023, a total of 68 SMRs relating to Cryptocurrency purchases were reported to FASU by the Financial Institutions (FIs) with an accumulated value of K4.47 million.



Graph 1: Transacted values against year and SMRs reported.

The transaction patterns across these SMRs (refer below in Graph 2), over the time period indicate that Visa Debit Cards are being used to purchase cryptocurrencies online from Cryptocurrency Brokers. 86.77% of the reported SMRs indicated international cryptocurrency brokers, with *Binance.com* being the most used cryptocurrency trading platform accounting for an accumulated value of K2.09m. Only 8.82% of the reported SMRs reported local, “commission-based” cryptocurrency facilitators (individuals), whom are primarily involved in aiding the exchange of cryptocurrencies and earning commissions in return (presumably in cryptocurrency). These local facilitators accounted for K0.76m in accumulated value for facilitating crypto purchases.

The FIs also reported undisclosed cryptocurrency brokers, that of which their activities have been vaguely reported or documented in the context of regulatory requirements for SMRs. These undisclosed brokers accounted for 4.41% of SMRs reported, with an accumulated value of K0.03m for facilitating crypto purchases.



Graph 2: Crypto brokers against total transacted values over the time period in which SMRs were reported.

Indicators of Cryptocurrency Transactions

According to the SMRs the following red flags are generally indicative of a cryptocurrency transaction:

1. Unusual transaction patterns; that are inconsistent with the customer's profile or previous transaction history & seem out of the ordinary. Transactions will be primarily done online using a visa card on a website that facilitates the brokerage of cryptocurrency.
2. Rapid movement of funds; for cryptocurrencies to multiple wallets or exchanges within a short period. Furthermore, the rapid conversion of cryptocurrencies to fiat currencies after acquisition.
3. Unexplained sources of funds; the inability of the customer to provide a legitimate source of funds for cryptocurrency purchases. Funds coming from unknown or unusual sources.
4. Inconsistent business activities; individuals or businesses engaging in crypto transactions that do not align with their stated business activities. A few SMRs reported company credit cards and accounts that are not in the crypto industry suddenly engaging in large-scale crypto transactions.

These indicators are not definitive proof of suspicious activity on their own, but rather red flags that would warrant further investigation.

Risk Patterns Identified

Cryptocurrency trading carries various risks due to its volatile nature, regulatory challenges, and potential for fraudulent activities. Here are some risk patterns commonly identified in cryptocurrency trading:

1. Lack of Regulation; Cryptocurrency markets often lack comprehensive regulation, exposing traders to potential scams, market manipulation, and lack of investor protection.
2. Hacking and Security Breaches; Cryptocurrency exchanges and wallets are frequent targets for cyberattacks. Traders risk losing their funds due to security vulnerabilities.
3. Ponzi Schemes and Scams; Unscrupulous individuals and organizations can create fraudulent schemes promising high returns, enticing traders to invest.
4. Tax and Legal Risks; Cryptocurrency trading can have tax implications that vary by jurisdiction, and traders might inadvertently violate local tax laws.
5. Investment Losses; Many cryptocurrencies and tokens have lost significant value over time, resulting in investment losses for traders and investors.

References

- Data-Flair. (2023, September 13). *Blockchain Cryptography – History | Cryptosystem*. Retrieved from <https://data-flair.training/blogs/blockchain-cryptography/>
- Khlebnikova, Y. (2023, September 13). *How can I open a bitcoin account?* Retrieved from Crypto News: <https://crypto.news/learn/how-can-i-open-a-bitcoin-account/>
- Merriam-Webster. (2023, September 12). *Merriam-Webster.com Dictionary*. Retrieved from <https://www.merriam-webster.com/dictionary/blockchain>
- wvaibhava. (2023, September 13). *Blockchain and Distributed Ledger Technology (DLT)*. Retrieved from Geeks for Geeks: <https://www.geeksforgeeks.org/blockchain-and-distributed-ledger-technology-dlt/>