INCIDENT REPORT FOR THEFT OF VIRTUAL ASSETS

[redacted]

CRYPTEGRIDY LTD Kemp House 160 City Road, EC1V 2NX

Investigator:	[redacted]
	CrypTegridy LTD
	Kemp House 160 City Road, EC1V 2NX
Subject:	Blockchain Incident Report
Offence:	Money Laundering, Fraud, Theft, organized crime activities
Accused:	Unidentified "organization members" "Actor" [redacted] "Actor" [redacted] "Actor" [redacted] "Actor" [redacted] "Entity" AML Association
Date of Request:	21/07/2022
Date of Conclusion:	15/08/2022
Report commissioned by:	[redacted] – [redacted]

Contents Page

Background to the Case

This case is related to a fraudulent broker website called orbitgtm-pros.com follows on from a case where the "victim" had 580800.24 EUR in both fiat and virtual assets stolen. In this case the "victim" claims they were defrauded by the accused using various "actors" representing the companies AML Association LTD and [redacted] By claiming that [redacted] has received a BTC transfer in the victim's name that has become stuck and payments for insurance and liquidity checks to the "accused" to release the stuck transfer of 1676448.00 (45.3369746 BTC) which matched the values shown on the victims orbitgtm-pros.com user dashboard. All asset transfers for fraudulent services take place on the Bitcoin blockchain.

1. Scope of the report

The scope of this report is limited to:

	Included in the report scope
1	Investigation of publicly available information of accused.
2	Collection of evidence related to the investigation.
3	Proof of ownership of stolen assets.
4	Tracking and tracing of stolen assets to withdrawal address.
5	Investigation of stolen BTC virtual asset on the Bitcoin blockchain.

2. Entities and evidence exhibits

[redacted] is referred to as the "victim."

The organization members are referred to as the "accused."

"[redacted] and "AML Association" – referred to individually as required.

All exhibits with the prefix "BA" are related to the "accused."

All exhibits with the prefix "HN" are related to the "victim."

All exhibits with the prefix "CT" are constructed by the "investigator."

Blockchain wallet addresses and transaction hashes have been abbreviated to seven digits, full addresses and transaction hashes can be referred to in the exhibit files.

	Exhibits submitted	
BA1	Email – mentioning OrbiGTM carefully leaving out the "t"	25.03.2022 Withdrawal Orbigtm.eml
BA2	Email – containing first documents from "accused"	07.04.2022 First document from AML Association about amount.eml
BA3	Email – request for insurance payment	09.05.2022 Re_ SV_ Corrected document.eml
BA4	Email – providing wallet address for insurance payment	25.05.2022 Info_1.eml
BA5	Email – claiming the "accused" are to cover half of the insurance	30.05.2022 Re_ Urgent - Question to be answered.eml
BA6	Email – "victim" claiming to have the remaining required to pay insurance	09.06.2022 Re_ The remaining installment EUR 66.500 now in [redacted] account.eml

BA7	Email – FAKE [redacted] finance team claiming the previous transaction is stuck and needs to be repeated	14.06.2022 Re_ [redacted] - Deposit for Declaration – HELP.eml
BA8	Email – the "victim" confirming another transfer	14.06.2022 Re_ BTC Withdrawal completed.eml
BA9	Email – "victim" shows an official [redacted] Support chat to the accused and is connected to a FAKE [redacted] AML compliance analyst	16.06.2022 AML Association connects to fake [redacted] actor.eml
BA10	Email – FAKE "[redacted] email provided and a request for liquidity check payment	17.06.2022 Re_ Email address for _[redacted] and [redacted] account for my wife.eml
BA11	Confirmation from "accused" those virtual assets "has been sent through" [redacted]	AML [redacted] pdf
BA12	"Accused" sent insurance contract first draft	AML Association Insurance.pdf
BA13	"Accused" sent insurance contract second draft	AML Association Insurance corrected.pdf
BA14	"Accused" liquidity check payment request	Liquidity Check [redacted] pdf
BA15	Email – "accused" requesting money through [redacted] bank account and [redacted]	05.07.2022 confirmation.eml
BA16	Email – "accused" increased the amount required to be sent by "victim"	05.07.2022 Corrected amount.eml
BA17	Email – "accused" request more payment for a [redacted] liquidity check	07.07.2022 Status of the withdrawal.eml
BA18	Email – further request for 838224.00 EUR for [redacted] liquidity check	08.07.2022 failed liquidity check of [redacted] eml
BA19	Email – "victim" questions the need for an additional [redacted] liquidity check	08.07.2022 Re_ SV_ failed liquidity check of [redacted] eml
BA20	Email – "accused" unable to postpone deadline	12.07.2022 case no.56859.eml
BA21	Email – "accused" enquiring about the transfer details for the liquidity check	18.07.2022 Liquidity check.eml
BA22	Email – "accused" again mentioning the deadline	18.07.2022 Liquidity check_1.eml
BA23	Email – "accused" sending more deadlines and fees	21.07.2022 Regarding Deadline.eml
BA24	Notice of [redacted] liquidity check from AML	Anti Money Laundering - [redacted] pdf
BA25	[redacted] liquidity check document	[redacted] [redacted] pdf
HN1	Email – [redacted] purchase confirmation	BTC purchase request confirmed.eml
HN2	Email – [redacted] purchase confirmation	BTC purchase request confirmed_1.eml
HN3	Email – [redacted] purchase confirmation	BTC purchase request confirmed_2.eml
HN4	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed.eml
HN5	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_1.eml
HN6	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_2.eml
HN7	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_3.eml

HN8	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_4.eml
HN9	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_5.eml
HN10	Email – [redacted] withdrawal confirmation	BTC withdrawal request confirmed_6.eml
HN11	[redacted] fiat transactions	fiat transactions record 20220801 182311.csv
HN12	[redacted] crypto transaction records	crypto transactions record 20220801 183059.csv
CT1	Flow chart of stolen virtual assets	Fake [redacted] AML Association.png
CT2	Flow of stolen virtual assets to various addresses in preparation for withdrawal on an exchange	Tracking of assets reported as stolen.xlsx
CT3	Transfers from the various addresses consolidated in alleged [redacted] controlled address	Custom Cluster of transfers of 1BnornP.xlsx
CT4	Transfers from the various addresses consolidated in alleged [redacted] controlled address	Custom Cluster transfers of 15MW833.xlsx
CT5	Transfers from the various addresses consolidated in alleged [redacted] controlled address	Custom Cluster transfers of 18tRbcp.xlsx
CT6	Transfers from the various addresses consolidated in alleged [redacted] controlled address	Custom Cluster transfers of 33A3b8v.xlsx
CT7	Transfers from the various addresses consolidated in alleged [redacted] controlled address	Custom Cluster transfers of 34X8wjx.xlsx
CT8	Transfer details of the “accused” sending stolen assets to multiple addresses in preparation for withdrawal on an exchange	Custom Cluster of transfers of bc1ql8k and bc1qu0g.xlsx
CT9	Fake AML Association LTD actor Reconnaissance	Fake AML Association LTD actor Recon.docx
CT10	Fake [redacted] actor Reconnaissance	Fake [redacted] actor Recon.docx

Further information required relative to the investigation

1	Information from [redacted] and [redacted] relating to the ownership of the following telephone number: [redacted] and it has paid business account for [redacted]
2	Information from [redacted] relating to the ownership of the email service provided to the owner of email [redacted]
3	Information from [redacted] relating to the ownership of the email or server service provided to the owner of email [redacted]
4	Information from any source relating to the ownership of the email or server service provided to the owner of email [redacted]
6	Report to be sent to law enforcement in relevant jurisdictions
8	Information from alleged exchange [redacted] relating to the ownership of the account of the received transfers by address ‘1BnornP...’ are sent transfers by the addresses in the file ‘Custom Cluster of transfers of 1BnornP.xlsx’ for further investigation by law enforcement

9	Information from alleged exchange [redacted] relating to the ownership of the account of the received transfers by address '15MW833...' are sent transfers by the addresses in the file 'Custom Cluster transfers of 15MW833.xlsx' for further investigation by law enforcement
10	Information from alleged exchange [redacted] relating to the ownership of the account of the received transfers by address '18tRbcp...' are sent transfers by the addresses in the file 'Custom Cluster transfers of 18tRbcp.xlsx' for further investigation by law enforcement
11	Information from alleged exchange [redacted] relating to the ownership of the account of the received transfers by address '33A3b8v..' are sent transfers by the addresses in the file 'Custom Cluster transfers of 33A3b8v.xlsx' for further investigation by law enforcement
12	Information from alleged exchange [redacted] relating to the ownership of the account of the received transfers by address '34X8wjx...' are sent transfers by addresses 'Custom Cluster transfers of 34X8wjx.xlsx' for further investigation by law enforcement

3. Evidence searched for

Evidence collected from the victim including correspondence emails, bank statements, virtual asset proof of ownership. Evidence gathered on publicly available data relating to the identities, phone numbers and email address domains.

4. List of Criminal Offence

The criminal offences facing the accused are:

Money Laundering, Fraud, Theft, organized crime activities

5. Breach

Use of social engineering to defraud the victim by making them pay for fake insurance and liquidity checks to release assets for withdrawal. No assets ever returned to the victim.

6. Investigation details

In this case I began by verifying the "victim's" ownership of the virtual asset Bitcoin (BTC) by checking the "victims" bank records and the [redacted] verification emails (exhibits HN1-HN3, HN11) as well as checking the [redacted] withdrawal verification records (exhibits HN4-HN10, HN12). The correspondence came from the "accused" representing the "AML Association" with regards to a OrbiGTM withdrawal (exhibit BA1), a fraudulent broker website the "victim" was also a victim of. By showing the "victim" fake documentation indicating the "AML Association" was responsible for returning a frozen amount 1676448.00 EUR (the same amount shown on the "victims" last login to the OrbitGTM platform) to affected individuals (exhibit BA2).

The "accused" went on to claim that the "victim" was an insured customer but had to make a payment for the insurance (exhibit BA3). Correspondence continues between the "victim" and the "accused" while details for on documents and amounts required to require for insurance payment. The "accused" claimed that after speaking with upper management they could offer a fifty percent discount and only "67,700.00 EUR worth of BTC" needed to be held on address 'bc1qd79…' for insurance payment (exhibit BA4). After the "victim" eventually paying 118000 EUR the "accused" still claimed another 66500.00 EUR was to be deposited (exhibit BA5). The "victim" paid the remaining balance to release the Bitcoin assets. All these transactions were made through the German Bank

[redacted] to [redacted] to send virtual assets to the address 'bc1qd79…' (Exhibit BA6) and were payment for insurance and liquidity check services (exhibits BA11-BA14). After paying for the insurance a fake "[redacted] representative began requesting liquidity payments to release an unauthorized transaction (exhibit BA7). After already gaining the victims trust the fake "AML Association" representative convinced the "victim" to pay another 1.467 BTC for a liquidity check (exhibit BA8).

After paying for the liquidity check the "victim" received an email form the fake "[redacted] representative saying the liquidity check had failed and the 1676448.00 EUR worth of BTC had been transferred back to the "AML Association." The "victim" the contacted the official "[redacted] support and was told that the email "[redacted] is not from us It is not official [redacted] domain from what I see in your account, there is no asset so please kindly report the case to the bank and the police in your country and also, I would like to provide you tips in order to avoid scams online." After forwarding the email to the fake "AML Association" representative the "accused" sent the fake details of a Sr. AML Compliance Analyst with the email address "[redacted] and all further correspondence from the "accused" I received as evidence was conducted using this email address (exhibit BA10).

The fake "[redacted] representative requested payment for "technical affairs" of 46000.00 EUR to be paid into the "victims" [redacted] account by using the German Bank [redacted] this amount was quickly corrected to 49000.00 EUR also mentioning [redacted] and [redacted] (exhibits BA15, BA16). The "accused" confirmed that the previous "transaction went through the verification" but there was more procedures and requirements to be completed before releasing the assets, one being a "[redacted] liquidity check included in the attached documents requesting payment of 40.9922794 BTC (838224.00 EUR) (exhibits BA17, BA24, BA25). The "victim" had no means to pay the 838224.00 EUR and was sent several emails with deadlines to pay before the assets were no longer available to be withdrawn. These deadlines have been extended in the hopes the "victim" can pay for the liquidity check (exhibits BA18-BA23).

By examining the on-chain data using a public blockchain explorer like Blockchain.com I was able to identify the "victims" 25.2897824 Bitcoin assets transferred from their [redacted] account to the address 'bc1qd79…' provided by the "accused". I then created a chart showing the flow of virtual assets (exhibit CT1). The virtual assets were the transferred to two address clusters 'bc1ql8k…' and 'bc1qu0g…' to be mixed with virtual assets accumulated by other means (exhibit CT8) and from there the virtual assets were scattered to obfuscate transfers to multiple addresses for preparation to be withdrawn on an exchange (exhibit CT2). The solen assets were then deposited into five addresses allegedly controlled by four different exchanges.

Stolen assets were deposited into address '1BnornP…' allegedly controlled by [redacted] (exhibit CT3).

Stolen assets were deposited into address '15MW833…' allegedly controlled by [redacted] (exhibit CT4).

Stolen assets were deposited into address '18tRbcp…' allegedly controlled by [redacted] (exhibit CT5).

Stolen assets were deposited into address '33A3b8v…' allegedly controlled by [redacted] (exhibit CT6).

Stolen assets were deposited into address '34X8wjx…' allegedly controlled by [redacted] (exhibit CT7).

Reconnaissance done on the email addresses and mobile phone number I found that the mobile phone service provider is EE in the UK, this phone number also has a paid business account on [redacted] (owned by [redacted] The service provider for the email address [redacted] is [redacted] and can be confirmed by resetting the password here https://maestro.[redacted] login. The serviced provider for the email address [redacted] is [redacted] (exhibits CT9, CT10)

7. Conclusion

- The "victim" has been defrauded of 25.2897824 BTC and 582260.13 EUR (at the time of purchase) by the accused
- I was able to track and trace the virtual assets to the alleged exchanges [redacted] and [redacted] which all have Know-Your-Customer and Anti-Money-Laundering Policies
- The virtual assets were mixed with other obtained virtual assets and transferred through various wallet addresses and deposited into the withdrawal addresses '1BnornP...', '15MW833...', '18tRbcp…', '33A3b8v…' and '34X8wjx…' controlled by the alleged exchanges previously mentioned
- Further investigation by law enforcement is required to reveal the identities of the accused from the available sources
- From the analysis of available evidence, the individuals responsible are a large well-organized group in overall control and should be taken very seriously

8. Generated Material

- Microsoft Word document of Fake [redacted] actor reconnaissance
- Microsoft Word document of Fake AML Association LTD actor reconnaissance
- Flow chart of stolen virtual assets image presented in .png format
- Seven Microsoft excel documents of assets traced to alleged centralized exchanges
- PDF printouts of all exhibits

9. **Glossary**

Address

A digital destination used to send and receive cryptocurrency funds. Cryptocurrency wallets can contain multiple addresses inside. Addresses vary depending on the specific blockchain it lives on.

Block

An entry of the cryptocurrency transactions that have been made in a certain time frame. A new block is validated approximately every 10 minutes on the Bitcoin network and becomes part of the blockchain. The blockchain is a sequence of connected data blocks.

Block Explorer

A website for viewing public blockchains and transaction information such as status and confirmation time. Blockchain.com and Etherscan.io are two examples of block explorers.

Bridge

Also known as a cross-chain bridge, a bridge allows the transfer of assets from one blockchain to another (e.g., Ethereum to Polygon). Bridges can be operated by a centralized entities or using a smart contract to facilitate the transfer in a decentralized process.

Cluster

A collection of cryptocurrency addresses that various data sources has been identified to be controlled by one entity.

Cold Wallet

A type of wallet that is not connected to the internet. This is also referred to as cold storage.

Counterparty

The other party that participates in a cryptocurrency transaction.

Custodial Wallet

A type of wallet in which a company or organization holds cryptocurrency assets and private keys on behalf of their users.

DAO

Also known as a decentralized autonomous organization, a DAO is an entity with no centralized decision makers. Instead, DAOs consist of a group of people who come together for a specific purpose without any one group or entity having full control. DAOs are built and run on a blockchain using smart contracts which defines the rules and protocols of the DAO.

Exposure

The relationship between addresses and other entities that is created through your transfers to and from other addresses. Exposure is a key component in measuring your risk levels.

Hosted Wallet

A wallet that resides on a third-party service, for example a centralized exchange. The third-party service may hold both the user's private and public keys.

Input

The cryptocurrency address from which funds were sent (the source of the coins in a single transaction). An input is also a reference to an output from a previous transaction.

Mining

The process by which transactions are validated and issued on the blockchain network. Miners receive a reward of cryptocurrency when they successfully add a block to the blockchain.

Mixing

Coin mixing could refer to any activity that involves the obfuscation of funds by substituting them with others. Coin mixing is commonly done by third party service providers for a fee. Multiple user assets are combined into one transaction and distributed. This can be done by hand for technically proficient users. The user will take all the information, craft it into a transaction, transfer to multiple addresses then collecting the assets in a wallet or service.

NFT

Also known as a non-fungible token, an NFT is unique code stored digitally on a blockchain. An NFT can only have one owner, and the owner is visible to everybody due to the public nature of blockchain technology. Users can purchase and sell NFTs using cryptocurrency on NFT marketplaces

Node

A participant in the blockchain network that verifies and stores transactions. There are multiple types of nodes that have distinct functions on varying blockchains.

Output

The cryptocurrency destination addresses for funds i.e., where funds are being sent. There can be multiple inputs and outputs for a single transaction.

Private Key

A secret alphanumeric string that allows the user to access the funds at a single corresponding address. Wallets contain one or more private keys.

Private Wallet

A type of wallet that allows the user to manage their own addresses and private keys.

Public Key

An alphanumeric string that is used to derive an address. The public key is only known if currency has been spent from its corresponding address.

Smart contract

Programs stored on a blockchain that run when predetermined conditions are met and verified. An example is a DEX (Decentralized Exchange) smart contract that facilitates the exchange of cryptocurrency between two people.

Transaction

A transaction consists of one or more fund transfers. On most blockchains a transaction comprises of a unique transaction ID (the transaction hash), inputs which are the source of the coins and outputs which are the destinations of the virtual assets.

Transaction Hash

Also known as a transaction ID, the transaction hash is a unique identifier of a transaction.

VASP

An acronym for Virtual Asset Service Provider.

Virtual Asset

The type of cryptocurrency used in a transfer (Bitcoin, Ethereum, USDT) Can also refer to non-fungible representations of value (e.g., NFTs).

Wallet

A software program that generates and stores a user's addresses and private keys. It is used to send and receive cryptocurrency and monitor balances.

10. All exhibits printed in .pdf