Coinfirm

AML Risk Report generated by Coinfirm's AML/CTF Platform (https://www.coinfirm.com).
ID: *19cea84363b0c1ed5239409b71953d8b94e6b73f2e5f86ab04c95dac0c9b246d*
Time: **2021-08-31T14:35:16.583Z** (UTC), Report Generation Block Height: **13133851**.
Refer to Terms of Service for conditions of Report use.

AML Risk Enhanced Report for ETH address

ce1f4b4f17224ec6df16eeb1e3e5321c54ff6ede

Unidentified

Address belongs to a hacker (Cream Finance exploit August 2021).

CURRENT BALANCE	5 758.582971 ETH
USD VALUE excl tokens	19 834 114.57 USD at 3444.27 USD/ETH rate
TOKENS	6 types
TOTAL INCL TOKENS	24 426 486.55 USD

C-SCORE ANALYSIS

LIST OF IDENTIFIED RISKS

- Address being a part of funds layering/mixing scheme related to hacked or misappropriated address
- Address belongs to hacker
- Address with part of incoming transactions in close proximity to obliged service with no KYC process
- Address with part of outgoing transactions in close proximity to obliged service with no KYC process
- Address with transactions incoming from new addresses
- Address with significant part of incoming transactions executed from new addresses
- Address with value peaks of outgoing transactions
- Address with significant part of incoming transactions the value of which is significantly higher than network average
- Address with high value current balance
- Address with at least one incoming transaction equal to or exceeding 15k EUR
- Address with significant part of single incoming transactions equal to or exceeding 15k EUR
- Address with at least one incoming transaction equal to or exceeding 10k USD
- Address with significant part of single incoming transactions equal to or exceeding 10k USD
- Address with dust funds tainted by incoming transactions from address belonging to decentralized exchange

PROFILE ANALYSIS

UNIDENTIFIED

OWNERSHIP INFORMATION

Name	Unidentified
Legal name	N/A

ADDRESS PROFILES

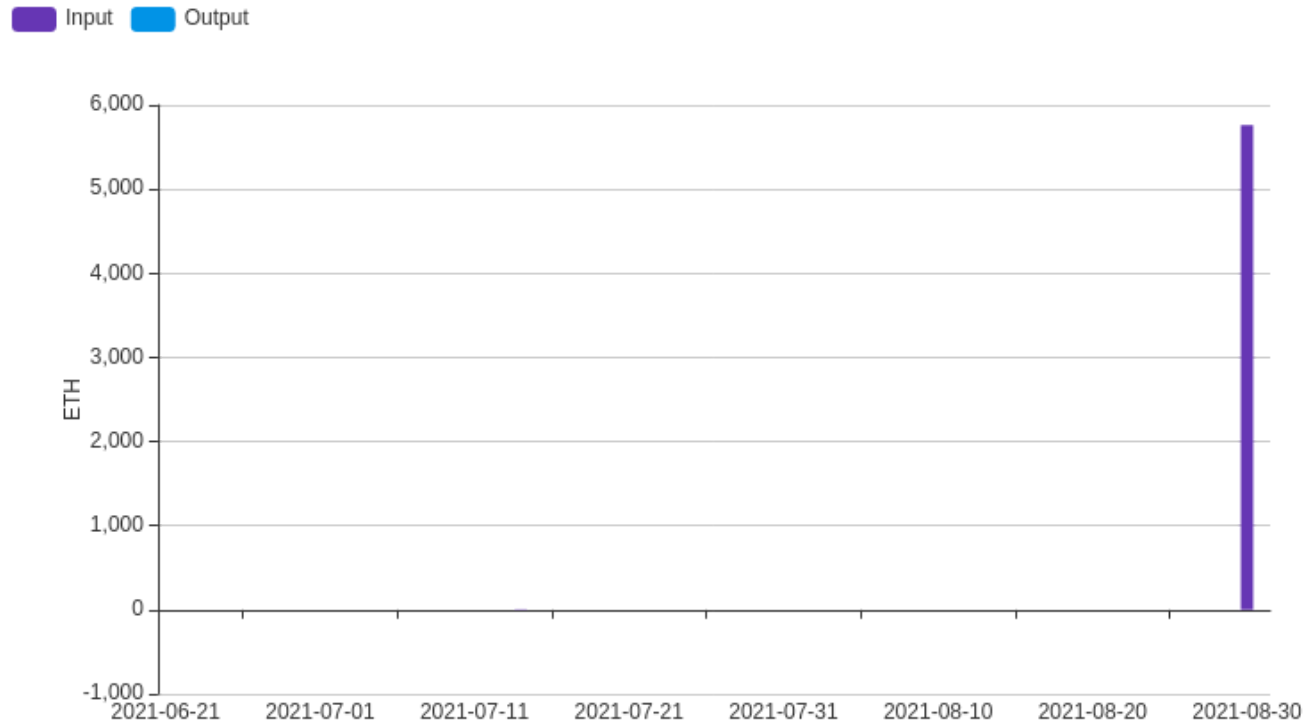
- Hacker

FINANCIAL ANALYSIS

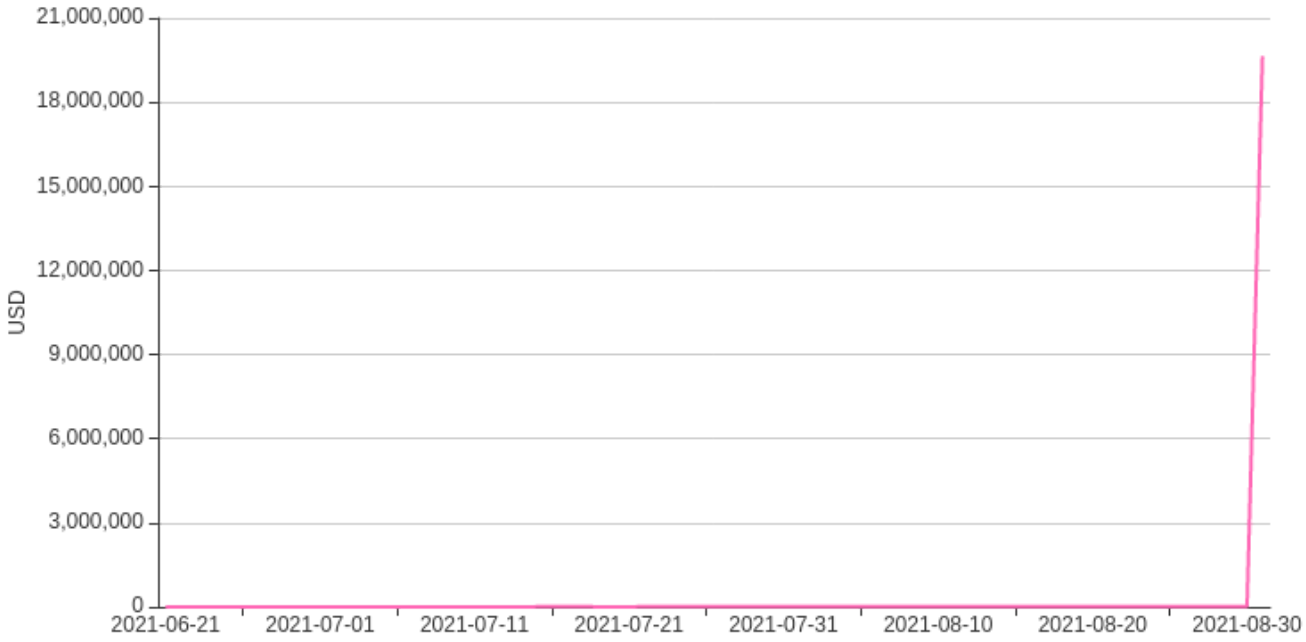
TOTAL TRANSACTIONS	128
TOTAL ETH TRANSFERS	131
ETH TURNOVER	5 765.904041 ETH $19 859 330.31

TOTAL ETH INPUT	5 765.897941 ETH $19 859 309.30	TOTAL ETH OUTPUT	0.0061 ETH $21.01
AVG ETH INPUT	240.245748 ETH $827 471.22	AVG ETH OUTPUT	0.000054 ETH $0.19
LARGEST	1 341.882675 ETH $4 621 806.24	LARGEST	0.004 ETH $13.78
SMALLEST	0 ETH $0.00	SMALLEST	0 ETH $0.00
ETH INPUT TRANSFERS	24	ETH OUTPUT TRANSFERS	113

INPUT / OUTPUT



ETH BALANCE

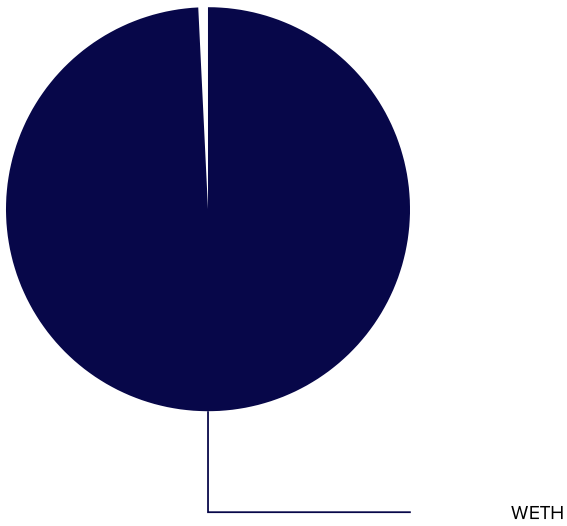


ASSETS

TOKENS THAT HAVE BEEN USED ON THIS ADDRESS.

SYMBOL	NAME	RATE (USD/TOKEN)	CURRENT BALANCE (IN TOKENS)	CURRENT VALUE (IN USD)
WETH	WrappedEther	3422.26	1 341.882675	$4 592 262.25
UNI	Uniswap	27.53	2.66048	$73.23
BUSD	BinanceUSD	0.999858	36.50586	$36.50
DAI	DaiStablecoin	1	0	$0.00
USDT	TetherUSD	1.01	0	$0.00
USDC	USDCoin	1	0	$0.00

TOKENS AMOUNT



 Informative

 Identified Risk

 Decreasing Factor

N/A Risk Verified But Not Identified

Money laundering

- N/A Industry risk - not a regulated activity
- N/A Charges and adverse media
- N/A High risk owner

No or limited KYC

N/A Address belongs to obliged service with no KYC process

N/A Address with significant part of incoming transactions in close proximity to obliged service with no KYC process

Address with part of incoming transactions in close proximity to obliged service with no KYC process

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an obliged service with no Know Your Client (KYC) process or account of its user; or
- The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an obliged service with no KYC process or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by an obliged service with no KYC process or account of its user;
- The evaluated blockchain address is discovered through data analysis as being owned (through ownership of private keys corresponding to this address) an obliged service with no KYC process or account of its user;
- An obliged entities such as digital currency exchanges, remittance companies, lending services or online cryptocurrencies wallets need to have a proper KYC process in place to meet regulatory requirements; lack of KYC process in obliged entities significantly increases the risk of using services of these entities for money laundering.

Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found through data analytics to be a deposit address of the cryptocurrencies exchange which does not require providing identity documents to activate the user's account and enable user's to trade unlimited volumes; the amount constituted a significant portion of funds incoming to the evaluated address.

N/A Address with significant part of outgoing transactions in close proximity to obliged service with no KYC process

Address with part of outgoing transactions in close proximity to obliged service with no KYC process

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds the significant percentage of which reach to the blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an obliged service with no Know Your Client (KYC) process or account of its user; or
- The evaluated blockchain address sends funds the significant percentage of which reach to the blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an obliged service with no KYC process or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by an obliged service with no KYC process or account of its user;
- The evaluated blockchain address is discovered through data analysis as being owned (through ownership of private keys corresponding to this address) an obliged service with no KYC process or account of its user;
- An obliged entities such as digital currency exchanges, remittance companies, lending services or online cryptocurrencies wallets need to have a proper KYC process in place to meet regulatory requirements; lack of KYC process in obliged entities significantly increases the risk of using services of

these entities for money laundering.

Example: The evaluated blockchain address sent the equivalent of USD 50 k which credited the addresses which were found through data analytics to be a deposit address of the cryptocurrencies exchange which does not require providing identity documents to activate the user's account and enable user's to trade unlimited volumes; the amount constituted a significant portion of funds outgoing from the evaluated address.

- N/A Address belongs to obliged service with limited KYC process
- N/A Address with significant part of incoming transactions in close proximity to obliged service with limited KYC process
- N/A Address with part of incoming transactions in close proximity to obliged service with limited KYC process
- N/A Address with significant part of outgoing transactions in close proximity to obliged service with limited KYC process
- N/A Address with part of outgoing transactions in close proximity to obliged service with limited KYC process
- N/A Address belongs to obliged service which had no KYC and currently has limited KYC process
- N/A Address belongs to obliged service which had no KYC and has implemented full KYC process
- N/A Address belongs to obliged service which had limited KYC and has implemented full KYC process

N/A Over the counter exchange

N/A Decentralized exchange

N/A DeFi service

N/A Increased risk entity

N/A Increased risk country

N/A Industry risk - regulated activity

N/A Transactions impeding track of funds - multiple input - multiple output transactions

Transactions impeding track of funds - new addresses transactions

- Address with transactions incoming from new addresses

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address receives funds from new blockchain addresses, which are the address with maximum one incoming transaction which occurred before the transaction executed to the evaluated address;
  - It is relatively more frequent in a group of users layering the track of funds to receive funds from new addresses, than it is in a group of random users.

- Address with significant part of incoming transactions executed from new addresses

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address receives significant value of funds from new blockchain addresses, which are the address with maximum one incoming transaction which occurred before the transaction executed to the evaluated address;
  - It is relatively more frequent in a group of users layering the track of funds to receive funds from new addresses, than it is in a group of random users.

- N/A Address with transactions outgoing to new addresses
- N/A Address with significant part of outgoing transactions executed to new addresses

N/A Transactions impeding track of funds - single incoming-outgoing transactions

N/A Transactions impeding track of funds - rapid movement of funds

N/A Transactions impeding track of funds - structuring payments

N/A Transactions impeding track of funds - passing funds through miners

N/A Transactions impeding track of funds - transactions impossible or difficult to decrypt

Transactions with distinctive patterns - high value addresses

- Address with high value current balance

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address has currently the balance of funds equal to or exceeding 1 Mil USD
  - It is relatively more frequent in a group of users involved in money laundering to achieve or maintain the high value balance of funds on the address, than it is in a group of random users.

- N/A Address with high value historic balance
- N/A Address maintaining high value balance for a long period of time

N/A Transactions with distinctive patterns - accumulating funds

N/A Transactions with distinctive patterns - dormant status

N/A Transactions with distinctive patterns - activity intervals

! Transactions with distinctive patterns - inconsistent transactions patterns

N/A Address with value peaks of incoming transactions

! Address with value peaks of outgoing transactions

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds in one or more transactions, the value of which is significantly higher than other transactions outgoing from this address; for example the evaluated blockchain address may have sent two transactions the value of each amounts to the equivalent of 500k USD at the exchange rate from the time of transactions, while there are 100 transactions outgoing from this address, with the maximum value equivalent to 500 USD;
- There is a significant number of transactions on the address;
- It is relatively more frequent in a group of users involved in illicit activities to send transactions the value of which is significantly higher than other transaction sent, than it is in a group of random users.

! Transactions with distinctive patterns - significant transactions value

! Address with significant part of incoming transactions the value of which is significantly higher than network average

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds in one or more transactions, the value of which is significantly higher than average value of transactions in blockchain network in the recent period; the value of such transactions constitutes a significant percentage of total transactions value received by the evaluated address; for example the evaluated blockchain address may have sent two transactions the value of each amounts to the equivalent of 500k USD at the exchange rate from the time of transactions, while the average value of transaction in blockchain network amounted to the equivalent of 1000k USD during the last 30 days;
- There is a significant number of transactions on the address;
- It is relatively more frequent in a group of users involved in illicit activities to sent transactions the value of which is significantly higher than average value of transaction in blockchain network in the recent period, than it is in a group of random users.

N/A Address with significant part of outgoing transactions the value of which is significantly higher than network average

N/A Transactions with distinctive patterns - significant transaction fees

N/A Transactions with distinctive patterns - round amounts

N/A Initial Coin Offerings issuers & beneficiaries

N/A Initial Coin Offerings contributors

N/A Restricted networks

- N/A Special addresses
- N/A Connected Parties
- N/A Staking
- N/A High risk exchanges

N/A Financing of terrorism and proliferation

! Direct links to crime and fraud offences

- N/A Weapon trade or trafficking
- N/A Crime against person
- N/A Drugs trade
- N/A Darknet markets
- N/A Ransom
- N/A Blackmail
- N/A Scams & investment frauds
- N/A Ponzi schemes
- N/A Pump and dump
- N/A Identity theft
- N/A intellectual property piracy
- N/A Credit card skimming or cloning
- N/A Tax evasion
- N/A Mixers & Tumblers
- N/A Deep web
- N/A Name of illicit activity
- N/A Shutdown or inactive service

N/A Cybercrime risk - ransomware

! Cybercrime risk - hacking & misappropriation

N/A Address which was hacked or misappropriated

! Address being a part of funds layering/mixing scheme related to hacked or misappropriated address

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address was discovered through data analysis with evidence or credible indication that it was used for the purpose of layering funds originating from a hack, exploit, or being misappropriated.

- Layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.
- Digital currency addresses of online services are frequently victims of hackings and misappropriation aimed to steal or misuse private keys required to sign and send blockchain transaction to the address managed by an illegitimate beneficiary.

N/A Address with significant part of incoming transactions in close proximity to addresses which were hacked or misapropriated

N/A Address with part of incoming transactions in close proximity to addresses which were hacked or misapropriated

N/A Address related to unauthorized withdrawal

N/A Address being a part of funds layering/mixing scheme related to unauthorized withdrawal

N/A Address with significant part of incoming transactions in close proximity to addresses related to unauthorized withdrawal

! Address belongs to hacker

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address was found or reported together with evidence or credible indication of being used by a hacker;
- The evaluated blockchain address is discovered through data analysis as being used by a hacker;
- While the term "hacker" can refer to any computer programmer, for the purpose of this risk indicator it should be considered as someone involved in illicit activity related to unwanted breaking into computer systems. The term “hacker” may also refer to a person or group being responsible for the execution of an exploit attack targeted at DeFi platforms or smart contracts. Exploit attack consists of exploiting the vulnerabilities in the technical structure of a blockchain system using the existing functions of the protocol, very often including the flash loan feature.

N/A Address with significant part of incoming transactions in close proximity to hacker's addresses

N/A Address with part of incoming transactions in close proximity to hacker's addresses

N/A Address with significant part of outgoing transactions in close proximity to hacker's addresses

N/A Address with part of outgoing transactions in close proximity to hacker's addresses

N/A Sanctions

N/A Bribery and corruption

AML reporting thresholds

AML reporting thresholds (EUR)

Address with at least one incoming transaction equal to or exceeding 15k EUR

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 15k EUR, at the exchange rate from the time of transaction;
- According to the existing regulations in certain jurisdictions such as European Union, each transaction the value of which equals to or exceeds 15k EUR, should be reported to the appropriate financial supervision authority.

Address with significant part of single incoming transactions equal to or exceeding 15k EUR

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 15k EUR, at the exchange rate from the time of transaction; the value of such transactions constitutes a significant percentage of total transactions value received by the evaluated address;
- According to the existing regulations in certain jurisdictions such as European Union, each transaction the value of which equals to or exceeds 15k EUR, should be reported to the appropriate financial supervision authority.

N/A Address with at least one outgoing transactions equal to or exceeding 15k EUR

N/A Address with significant part of single outgoing transactions equal to or exceeding 15k EUR

AML reporting thresholds (USD)

Address with at least one incoming transaction equal to or exceeding 10k USD

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 10k USD, at the exchange rate from the time of transaction;
- According to the existing regulations in certain jurisdictions such as United States, each transaction the value of which equals to or exceeds 10k USD, should be reported to the appropriate financial supervision authority.

Address with significant part of single incoming transactions equal to or exceeding 10k USD

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 10k USD, at the exchange rate from the time of transaction; the value of such transactions constitutes a significant percentage of total transactions value received by the evaluated address;
- According to the existing regulations in certain jurisdictions such as United States, each transaction the value of which equals to or exceeds 10k USD, should be reported to the appropriate financial supervision authority.

N/A Address with at least one outgoing transactions equal to or exceeding 10k USD

N/A Address with significant part of single outgoing transactions equal to or exceeding 10k USD

Dust funds taint

- N/A Terrorism financing
- N/A Weapon trade or trafficking
- N/A Crime against person
- N/A Drugs trade
- N/A Darknet markets
- N/A Ransom
- N/A Blackmail
- N/A Scams & investment frauds
- N/A Ponzi schemes
- N/A Pump and dump
- N/A Identity theft
- N/A Intellectual property piracy
- N/A Credit card skimming or cloning
- N/A Tax evasion
- N/A Mixers & Tumblers
- N/A Deep web
- N/A Cybercrime risk - ransomware
- N/A Cybercrime risk - hacking & misappropriation

High risk exchanges

N/A Address with dust funds tainted by incoming transactions from address belonging to over the counter exchange

Address with dust funds tainted by incoming transactions from address belonging to decentralized exchange

This risk indicator does not increase the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by a decentralized exchange or account of its user; or
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an over the counter exchange or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by a decentralized exchange or account of its user;
- Decentralized exchanges are trading services allowing for direct trade between two parties, without the supervision of an exchange, frequently involving cash transactions;
- Decentralized exchanges are considered as entities with AML increased risk according to most of the related regulations; decentralized exchanges are considered as obliged institutions according to the AML FATF guidelines, EU directives and multiple other jurisdiction-specific regulations; decentralized exchanges are frequently used in money laundering as they act at the intersection of cryptocurrencies and traditional financial system and allow for greater anonymity than regular digital currency exchanges.

Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found on deep web forum to be a deposit addressed of peer-to-peer cryptocurrencies exchange service advertising as an exchange providing outstanding anonymity of it\'s users; the pattern of transactions tree of the service was discovered through data analytics to be characteristic for large scale peer-to-peer exchange of cryptocurrencies; the amount constituted a significant portion of funds incoming to the evaluated address.

N/A No or limited KYC

N/A Sanctioned country subject

N/A Sanctioned subject

N/A Politically exposed person (PEP)

N/A Blacklists and Whitelists

N/A Risk decreasing factors

APPENDIX 2

LAST 3 MONTHS

TOTAL TRANSACTIONS	128
TOTAL ETH TRANSFERS	131
TURNOVER	5 765.904041 ETH $19 859 330.31

TOTAL ETH INPUT	5 765.897941 ETH $19 859 309.30	TOTAL ETH OUTPUT	0.0061 ETH $21.01
AVG ETH INPUT	240.245748 ETH $827 471.22	AVG ETH OUTPUT	0.000054 ETH $0.19
LARGEST	1 341.882675 ETH $4 621 806.24	LARGEST	0.004 ETH $13.78
SMALLEST	0 ETH $0.00	SMALLEST	0 ETH $0.00
ETH INPUT TRANSFERS	11	ETH OUTPUT TRANSFERS	120

LAST 6 MONTHS

TOTAL TRANSACTIONS	128
TOTAL ETH TRANSFERS	131
TURNOVER	5 765.904041 ETH $19 859 330.31

TOTAL ETH INPUT	5 765.897941 ETH $19 859 309.30	TOTAL ETH OUTPUT	0.0061 ETH $21.01
AVG ETH INPUT	240.245748 ETH $827 471.22	AVG ETH OUTPUT	0.000054 ETH $0.19
LARGEST	1 341.882675 ETH $4 621 806.24	LARGEST	0.004 ETH $13.78
SMALLEST	0 ETH $0.00	SMALLEST	0 ETH $0.00
ETH INPUT TRANSFERS	11	ETH OUTPUT TRANSFERS	120

LAST 12 MONTHS

TOTAL TRANSACTIONS	128
TOTAL ETH TRANSFERS	131
TURNOVER	5 765.904041 ETH $19 859 330.31

TOTAL ETH INPUT	5 765.897941 ETH $19 859 309.30	TOTAL ETH OUTPUT	0.0061 ETH $21.01
AVG ETH INPUT	240.245748 ETH $827 471.22	AVG ETH OUTPUT	0.000054 ETH $0.19
LARGEST	1 341.882675 ETH $4 621 806.24	LARGEST	0.004 ETH $13.78
SMALLEST	0 ETH $0.00	SMALLEST	0 ETH $0.00
ETH INPUT TRANSFERS	11	ETH OUTPUT TRANSFERS	120

FIRST INCOMING TRANSACTION

TRANSACTION HASH	b3d9fc384a146c385df30a8ce401ad44437e5fc96efcee911afdedfd2836d810
BLOCK TIME	21.06.2021 16:13:47
BLOCK HEIGHT	12678641
TRANSACTION AMOUNT	0.05 ETH
TRANSACTION USD VALUE	$99.66

FIRST OUTGOING TRANSACTION

TRANSACTION HASH	13d444f3b49e73e6c86e3ed9994f853a2463d0e08de2ad7f29706ab6f921f37b
BLOCK TIME	21.06.2021 16:19:53
BLOCK HEIGHT	12678667
TRANSACTION AMOUNT	0 ETH
TRANSACTION USD VALUE	$0.00

LAST INCOMING TRANSACTION

TRANSACTION HASH	79c9e51470ee3f75754ebcfd8383c8b3e32659f4e71c8e99cc59db67482e55a4
BLOCK TIME	30.08.2021 10:10:55
BLOCK HEIGHT	13126246
TRANSACTION AMOUNT	0.00001 ETH
TRANSACTION USD VALUE	$0.03

LAST OUTGOING TRANSACTION

TRANSACTION HASH	55f05724757fba1247a99a8b1d11dc0f902c07d91291e3b2531b7921ecb47fc5
BLOCK TIME	30.08.2021 06:29:43
BLOCK HEIGHT	13125262
TRANSACTION AMOUNT	0 ETH
TRANSACTION USD VALUE	$0.00

LAST 24 HOURS ACTIVITY

INFLOW	0 ETH
OUTFLOW	0 ETH
AVERAGE INFLOW	0 ETH
AVERAGE OUTFLOW	0 ETH

DISCLAIMER

The Report is information only and is valid on the date of its issuance. Coinfirm does not give any express or implied warranty to the validity of any Report after the date of issuance of any Report.

Coinfirm takes all steps necessary to provide an independent analysis and information in the Report.

Coinfirm is not liable for any changes in assumptions and updates to this report in the case of new facts or circumstances occurring after the date of the Report or not known to Coinfirm at the time of generation of this Report.

Any decision taken by the recipient of this report is made solely on their own risk. The liability of Coinfirm is hereby excluded to the fullest extent permitted by the applicable law. The Report does not discharge any obligation of proper internal risk assessment and/or decision making process.

In no event will Coinfirm be liable to the recipients for:

- any act or alleged act, or any omission or alleged omission, that does not constitute wilful misconduct by Coinfirm, as determined in a final, non-appealable judgment by a court of competent jurisdiction,
- any indirect, special, punitive, incidental, exemplary, expectancy or consequential damages, including lost profits, lost revenues, loss of opportunity or business interruption, whether or not such damages are foreseeable, or
- any third-party claims (whether based in statute, contract, tort or otherwise).

This report should be read in full because any separate analysis of each of its parts can lead to erroneous conclusions.

Certain information, due to high risk (e.g. crime related), used for analysis, may not be able to be disclosed to the recipient.

To clarify any aspects contained in the Report please contact us at report@coinfirm.com.

GLOSSARY

Address	an address is like a bank account and for example a Bitcoin address starts with either a ‘1’ or a ‘3’ or a ‘bc1’ and is 26-35 alphanumeric characters in length. The address is generated from the private key, which is required to move assets assigned to this address to another address(es).
Anti-Money Laundering (AML)	the process of systems and controls that are applied to deter, disrupt and detect the flow of illicit value between collusive criminals that represents the proceeds of crimes and predicate offences such as tax evasion, sanctions evasion, theft, counterfeiting and fraud.
Blockchain	is a public ledger that records transactions that are performed. This is achieved without any trusted central authority as the maintenance of the blockchain is performed by a network of communicating nodes running the software. Network nodes validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.
Combating the Financing of Terrorism (CFT)	the process of deterring and disrupting the financing of terrorism and proliferation. It is increasingly difficult to distinguish from money laundering activity due to the collusive conduct of terrorist financiers and transnational organized criminals, but it is typically distinguished from money laundering on the grounds that the sources of money laundering must be criminal, whereas the sources of finance for terrorism include donations from lawfully earning income. The goal of money laundering is typically a financial gain, while the goal of terrorism financing is typically ideological activity.
Customer Due Diligence (CDD)	a process to assess all of the risks associated with a client or relationship, including KYC, and that requires that the overall client conduct, and transactions are assessed to determine if this is unusual and reportable. CDD requires that obliged entities assess the risks before entering in to a relationship, and continuously thereafter in response to trigger events or suspicious activity for example. It is a continual process that is designed to assess and monitor changes in customer risks.
Decentralised Virtual Currencies	(cryptocurrencies) are distributed, open-source, mathematically-based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include: Bitcoin, Ethereum, Litecoin and Namecoin.
Distributed Ledger (Shared Ledger)	‘Ledgers’, or put simply, records of activity, were historically maintained on paper, more recently these were transferred to bytes on computers, and are now supported by algorithms in blockchains. They are essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the

	ledger are maintained cryptographically using ‘keys’ and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network. (Taken from UK Government: ‘Distributed Ledger Technology: beyond block chain’).
Electronic money (e-money)	is an electronic store of monetary value, based on technological mechanism for holding and accessing fiat currency.
Enhanced Customer Due Diligence (EDD)	a higher standard of due diligence, including identity verification and investigation that is required to be performed for those clients and relationships that have been identified as presenting the greatest risk of financial crimes. These risks include among others PEPs, Correspondent Banking, non-face-to-face activities such as virtual currency and private banking.
Exchanger / virtual currency exchange	is a website service, or an entity, engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wire payments, credit cards, and other virtual currencies. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts. Examples include: Bitstamp, GDAX, Kraken, OKCoin and ItBit.
Fiat Currency	is legal tender that is backed by the central government who issued it. Examples are the US Dollar, Japanese Yen and UK Sterling.
‘Fifth’ EU Money Laundering Directive (5MLD)	an amendment to the 4MLD that was agreed in response to the terrorist attacks across Europe in 2015 and 2016. The new law must be transposed by member states by 10th January 2020, and new measures include the requirement for virtual currency exchange services and virtual currency custodian wallet providers to be treated as ‘obliged entities’.
FinTech	refers to new applications, processes, products or business models that are being applied to improve the efficiency and security of financial services.
Fourth EU Money Laundering Directive (4MLD)	European response to the FATF 40 Recommendations from February 2012 and was required to be transposed by EU member states by 26th June 2017.
Hash	A hash value (or simply hash), also called a message digest, is a string of characters generated from a string of digital data, e.g. a pdf file. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value and it is extremely difficult to reverse to identify the source message.

Know Your Customer (KYC)	the identification and verification of the natural person, legal entity or legal arrangement through identifying information, such as name and address, and the verification of these details to identify fraud, misrepresentation etc.
Money Laundering	a process to disguise the illicit source of value, either by self-laundering or through the placement, layering or integration process, conducted by criminals who ultimately wish to use this value for self-gratification, or to continue to finance their illicit activities.
Money Laundering Reporting Officer (MLRO)	the chief compliance officer responsible for all AML/CFT activities and responsible for ensuring that an obliged entity is not used by criminal or the financiers of terrorism.
Nodes	are computers in the blockchain network which receive new transactions and blocks, validate these transactions and blocks and spread valid transactions and blocks to connected nodes and ignore invalid transactions and blocks. It is generally considered that the more nodes exist in the network, the more secure the is the system.
Politically Exposed Person (PEP)	a person of high public office who may be able to influence the misappropriation of public funds whilst in office, or the awarding of public contracts. Include members of government, ruling classes such as Presidents, Royalty, Ministers of the Government and military and judiciary. The families of PEPs, and their close business associates, are also included due to the close affinity and trust that they may enjoy in their relationship, and which may lead to the PEP using these relationships as ‘front’ or ‘informal’ nominees.
Private Key	a private key is a cryptographic code that functions as a secret password that allows the user to sign a cryptocurrency transaction and transfer funds to another cryptocurrency address. Using the private key proves ownership of cryptocurrency.
Sanctions	when applied to financial services, represent a prohibition on providing regulated services to the subject of the sanction, and the requirement to freeze and report any assets that are held to the local jurisdiction sanctions administrator, such as OFAC or HMT.
Simplified Due Diligence (SDD)	a lower level of customer due diligence verification that can be performed where there is no, or a lesser, risk of money laundering.
Trading platforms	function as marketplaces, bringing together buyers and sellers of virtual currencies by providing them

	with a platform on which they can offer and bid among themselves. In contrast to exchanges, the trading platforms do not engage in the buying and selling themselves. Some trading platforms give their customers the option of locating potential customers nearby. Examples include LocalBitcoins.com and Mycelium Local Trader.
Transaction Fee	Is earned by miners when a transaction is completed. The minimum transaction fee required is determined by the "size" (kilobytes) of the transaction data. Most small transactions require a fee of about 0.0001 BTC and transactions with larger fees are given priority to be added to the block, so they are usually confirmed faster than transactions with low fees.