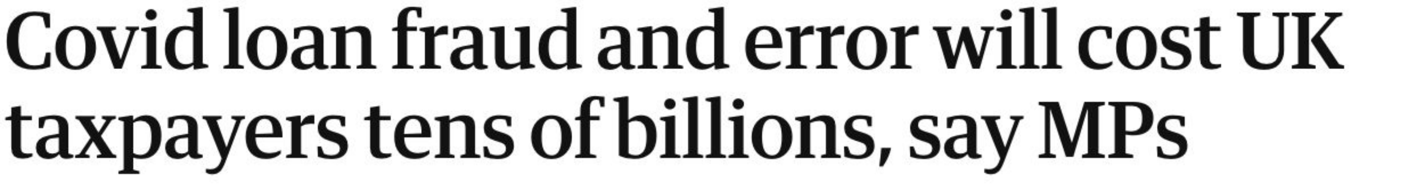
Chainalysis

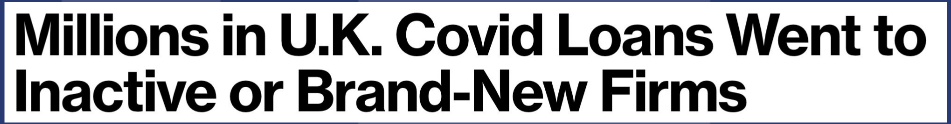
Benefit Fraud Investigations

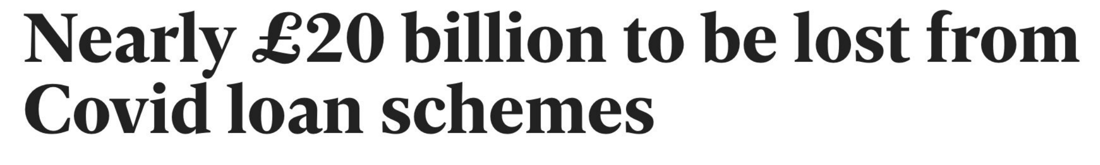
with enhanced blockchain analytics

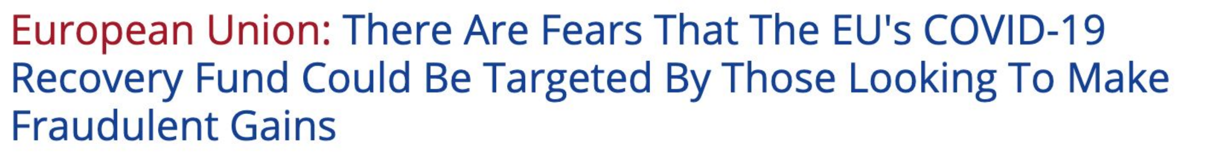
December 2021

Overview

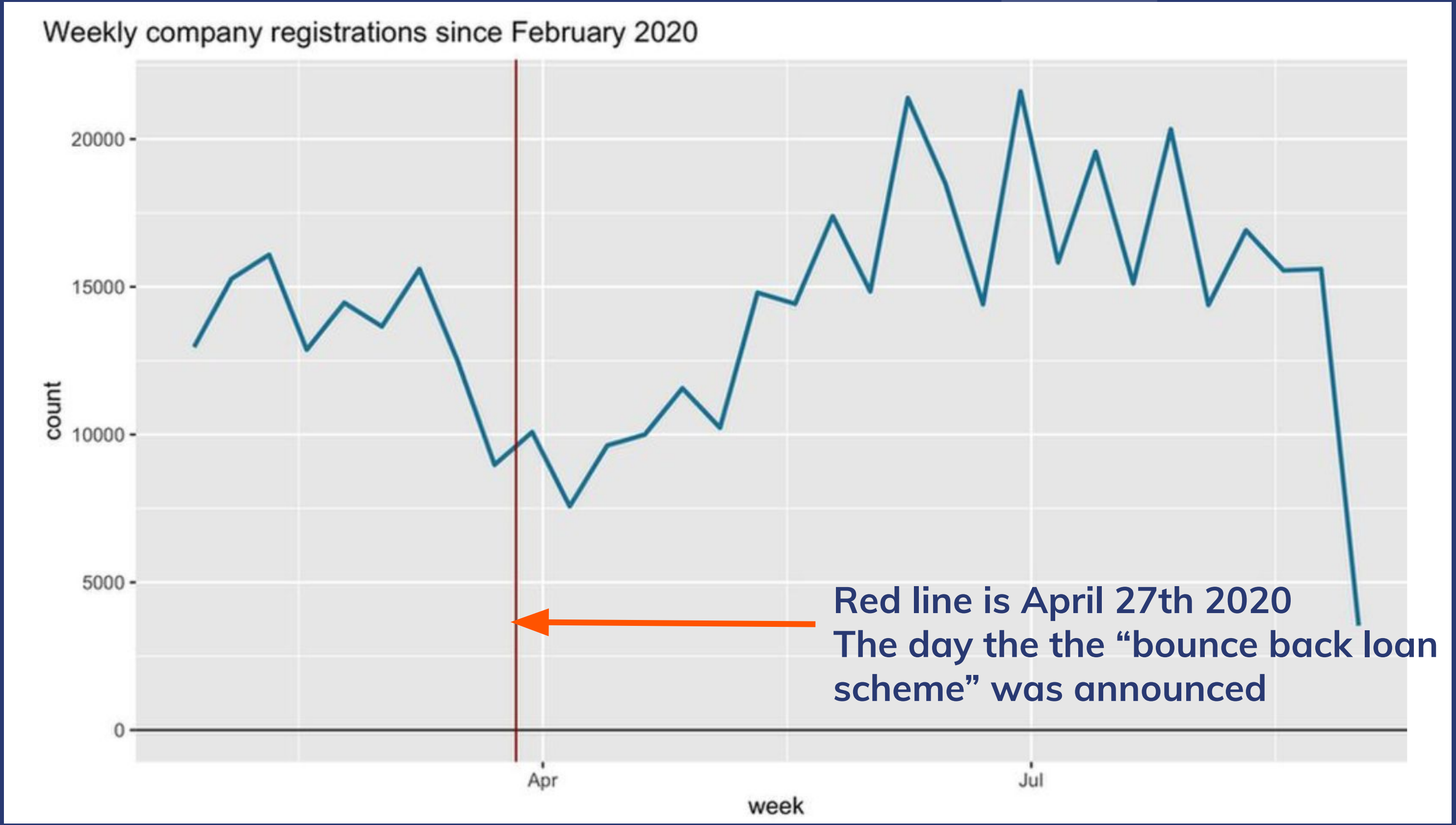

Covid loan fraud and error will cost UK taxpayers tens of billions, say MPs


Millions in U.K. Covid Loans Went to Inactive or Brand-New Firms


Nearly £20 billion to be lost from Covid loan schemes


European Union: There Are Fears That The EU's COVID-19 Recovery Fund Could Be Targeted By Those Looking To Make Fraudulent Gains

Overview



Red line is April 27th 2020
The day the the “bounce back loan scheme” was announced

Overview

Situation Fraudulently obtained welfare payments converted and laundered through cryptocurrency.

Objective Identify methodologies and financial impacts of the fraudulent conduct and establish the destination of funds. (crypto to fiat off ramps).

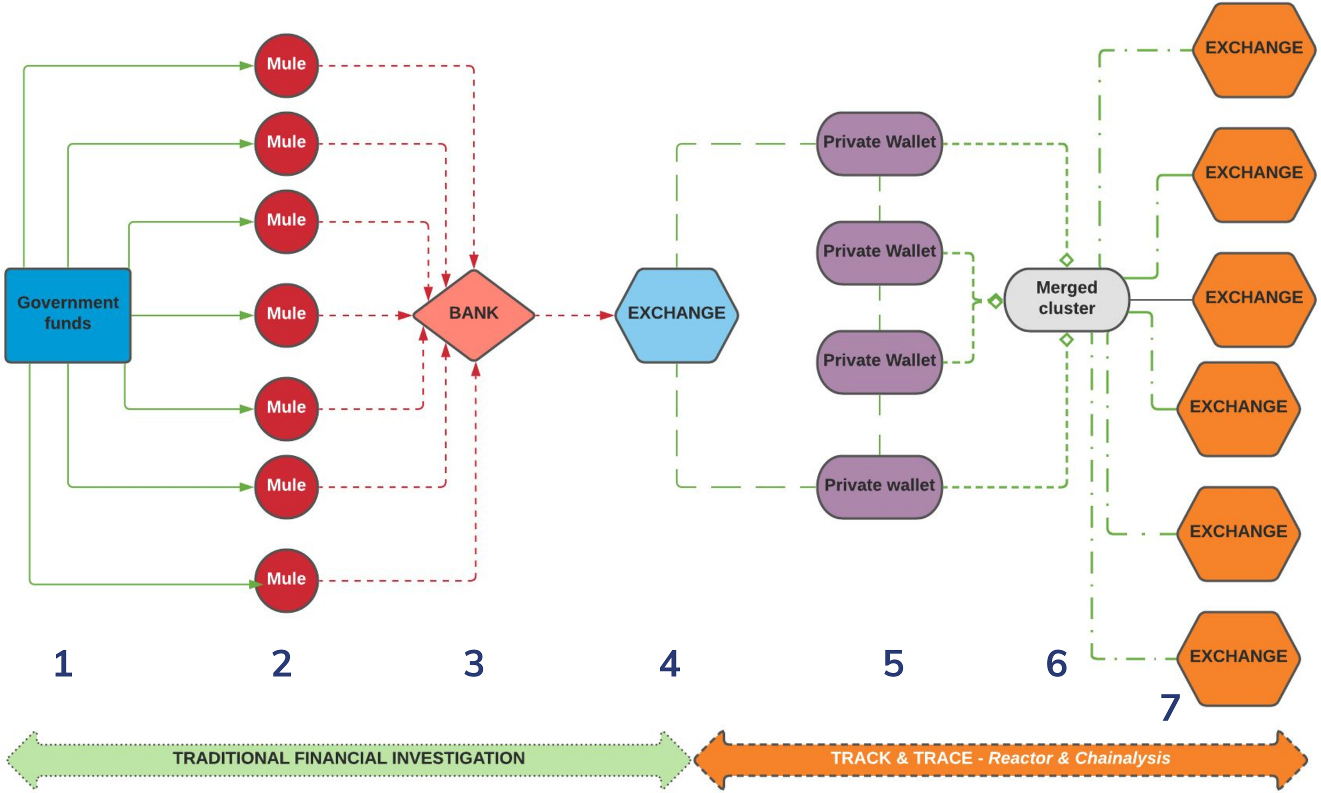
Action Investigate the flow of cryptocurrency (chainalysis solutions), provide target development and analytical support.

Result Identify the illicit structure of funds used by OCG and the proceeds of crime.

Start Point

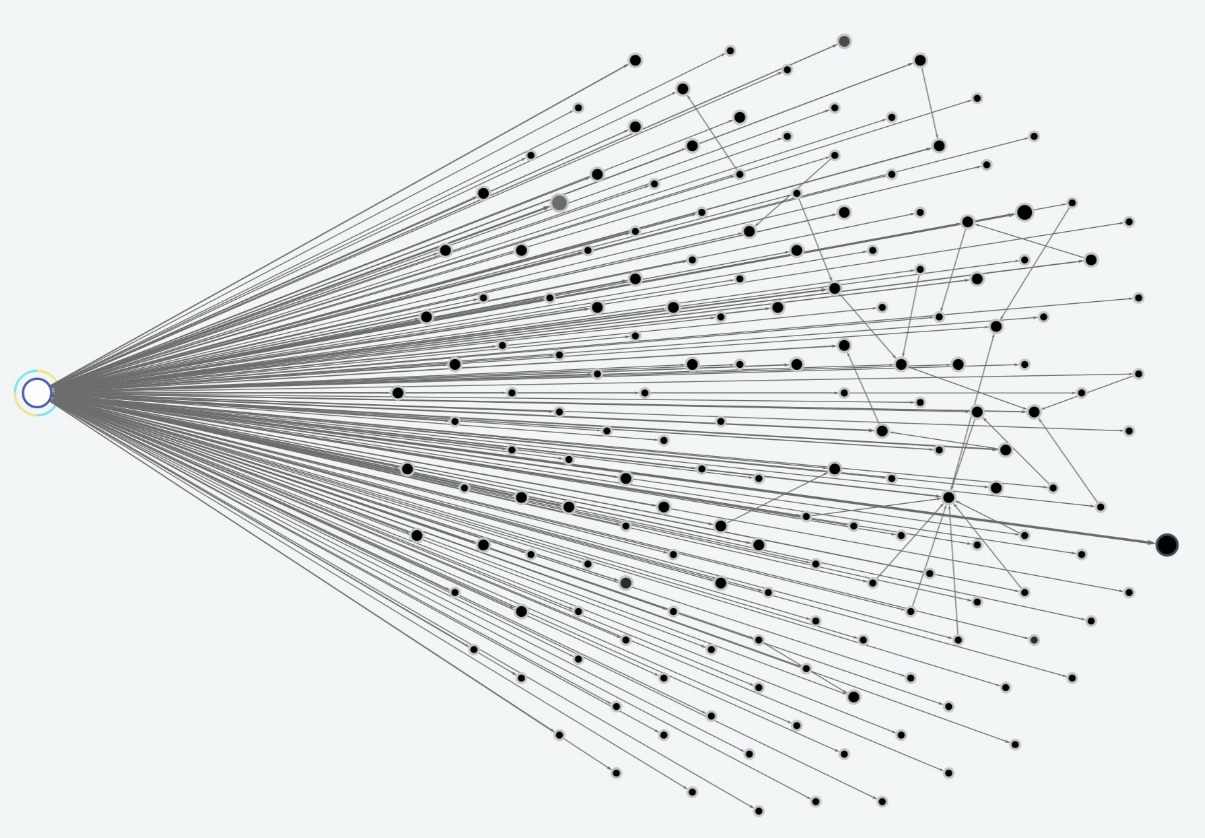
- Initial start point was fraudulently obtained government funds
- These funds are paid to a network of ***mule*** bank accounts
- The mules are provided with instructions to convert the ***fiat*** (government-issued currency) to cryptocurrency
- Signposted to use ***Exchange 1*** for the conversion
- Traditional financial investigation used to identify the mule accounts and to establish who has sent or received funds from any known cryptocurrency exchange (predominantly Coinbase)
- Engage with ***Exchange 1*** to identify where received funds were then sent
- Use **Reactor** to ***track and trace*** funds and to identify other members of the OCG and links to other criminally derived cryptocurrency holdings

The workflow



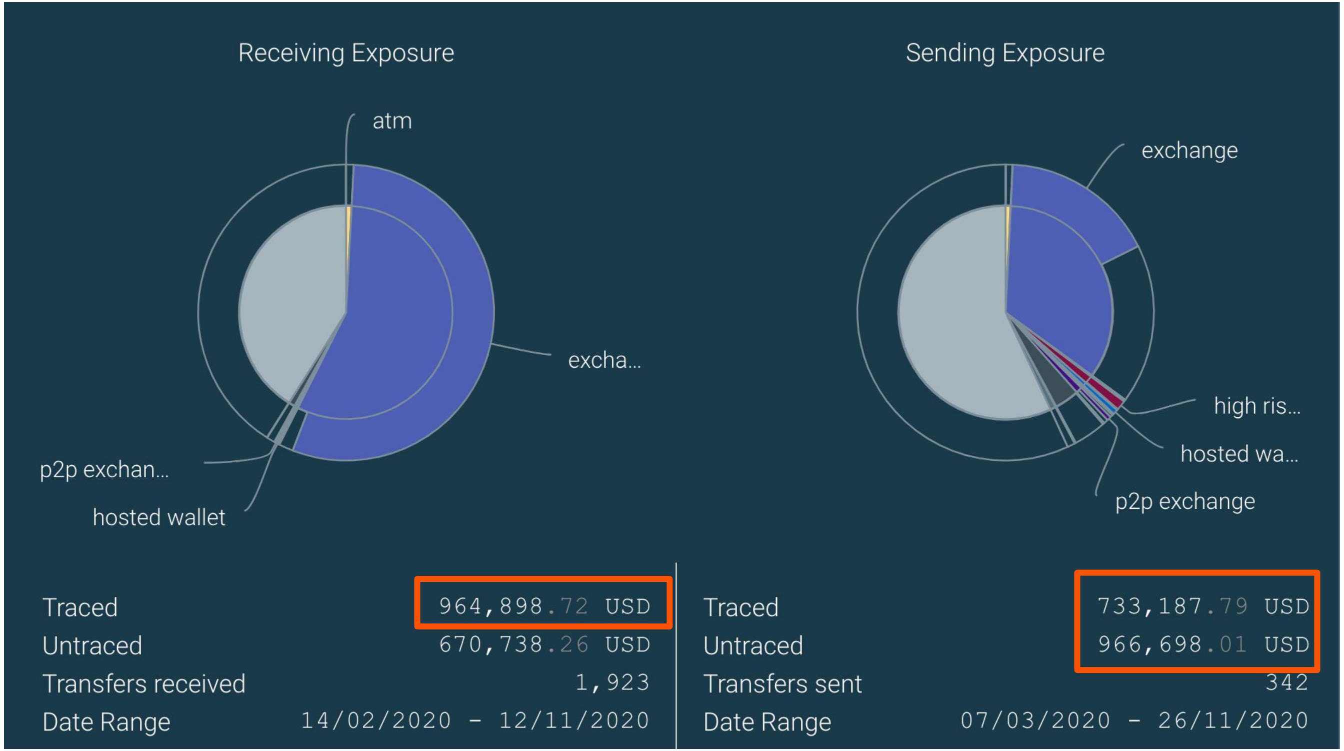
1. Gov funds are sent
2. Funds received by network of mules
3. Funds paid into bank accounts
4. Funds then sent to designated deposit address at exchange
5. Funds then transferred to series of private wallets
6. Private wallets are then merged and treated as one to determine end destination
7. Cash out points

The data



- All withdrawals from *Exchange 1* identified
- 175 separate transactions
- Bulk of these withdrawals are to private wallets
- 11 withdrawals direct to further deposit addresses at exchanges

The data: consolidation point

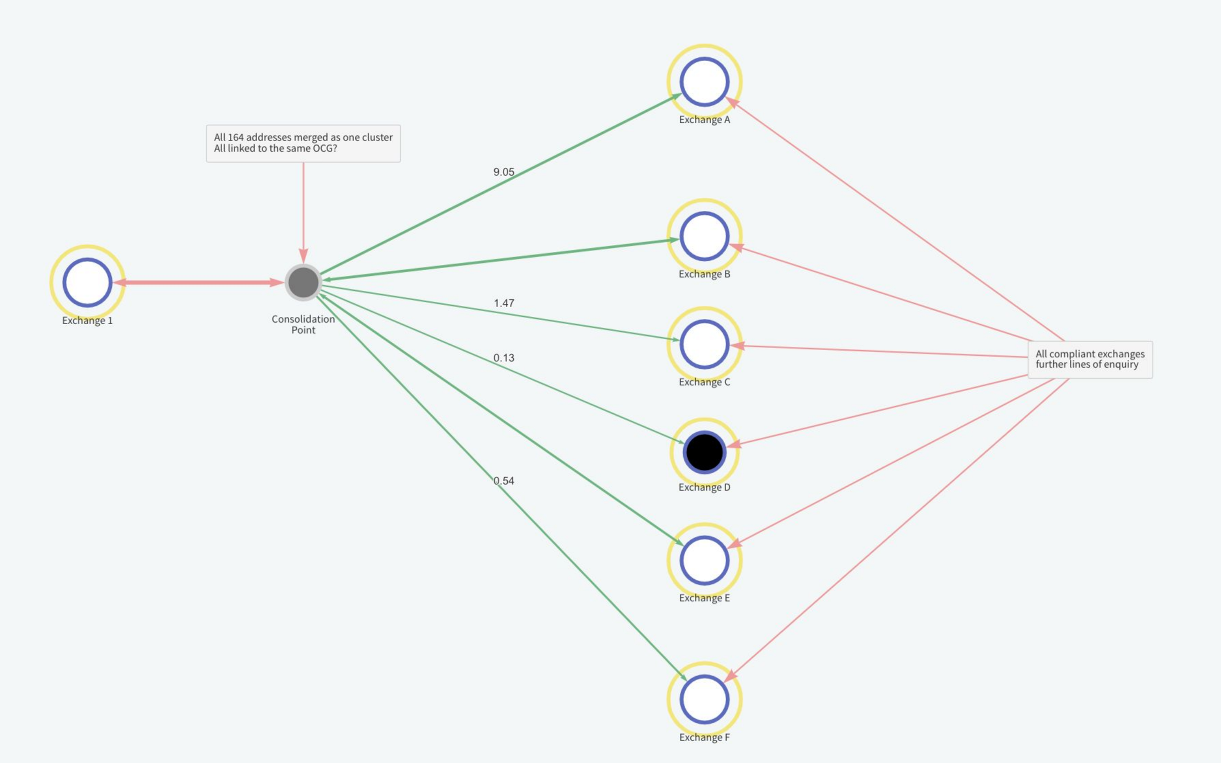


Traced	964,898.72 USD
Untraced	670,738.26 USD
Transfers received	1,923
Date Range	14/02/2020 - 12/11/2020

Traced	733,187.79 USD
Untraced	966,698.01 USD
Transfers sent	342
Date Range	07/03/2020 - 26/11/2020

- **All 164 receiving addresses have been *merged***
- **Total received is $964K**
- **56% of funds have come directly from Exchange 1**
- **There is also significant *indirect* exposure from Exchange 1 which may identify other persons involved in this fraud**

The data - the off ramps

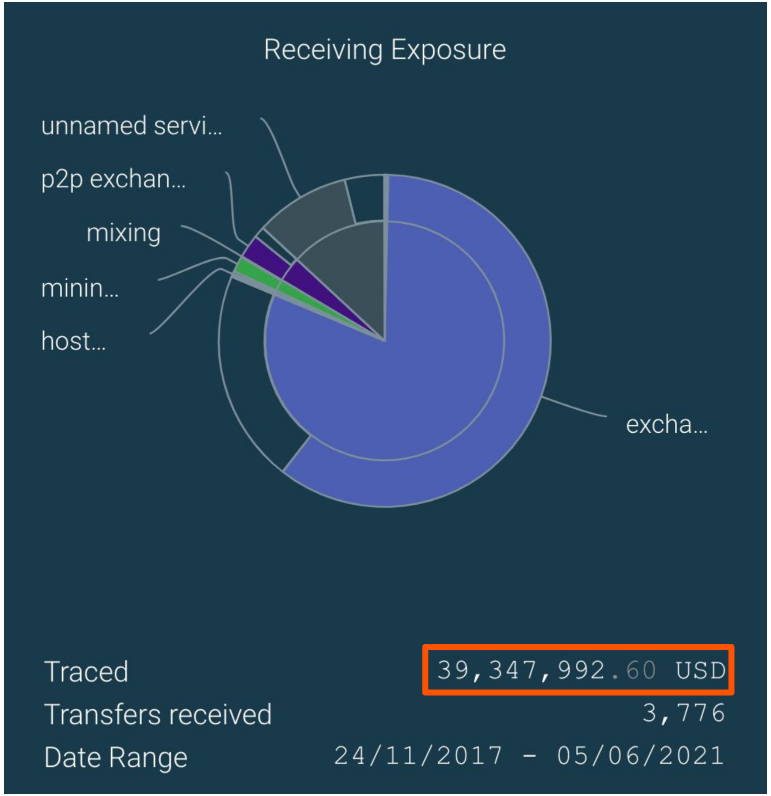

All 164 addresses merged as one cluster
All linked to the same OCG?
Exchange 1
Consolidation Point
9.05
1.47
0.13
0.54
Exchange A
Exchange B
Exchange C
Exchange D
Exchange E
Exchange F
All compliant exchanges further lines of enquiry

- The simplest workflow to identify where funds are cashed out or the *off ramps* are to identity direct sending exposure to compliant exchanges
- 6 major Exchanges have received the bulk of these funds
- The sending exposure provides a quick visual guide as to the breakdown of where funds have been sent

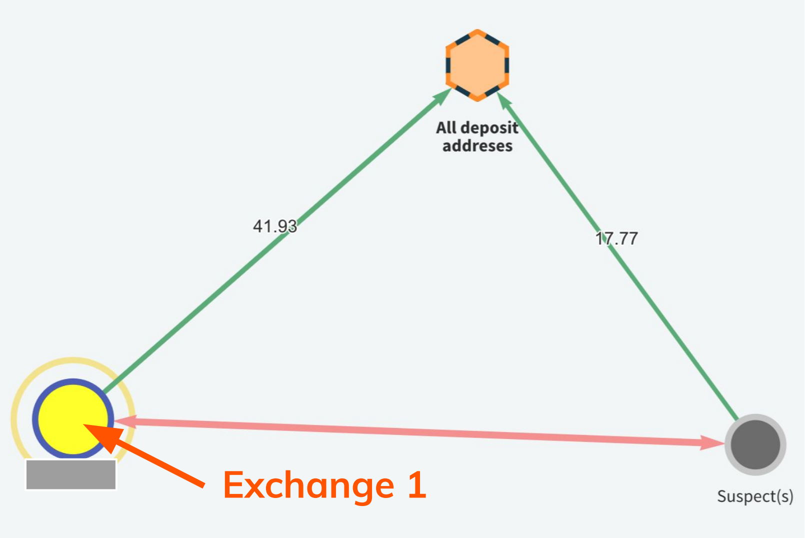
The data: isolating deposit addresses

Exchange	Total amount	Date range	TXs
Exchange A	**$38 million**	**09/09/2018 - 16/10/2020**	**3526**
Exchange B	**$413,000**	**03/11/2020 - 05/06/2020**	**23**
Exchange C	**$491,000**	**24/11/2017 - 20/05/2020**	**32**
Exchange D	**$13,800**	**05/06/2020 - 16/07/2020**	**8**
Exchange E	**$506,000**	**19/04/2020 - 06/09/2020**	**97**
Exchange F	**$62,000**	**10/05/2020 - 10/12/2020**	**60**

The data: isolating deposit addresses

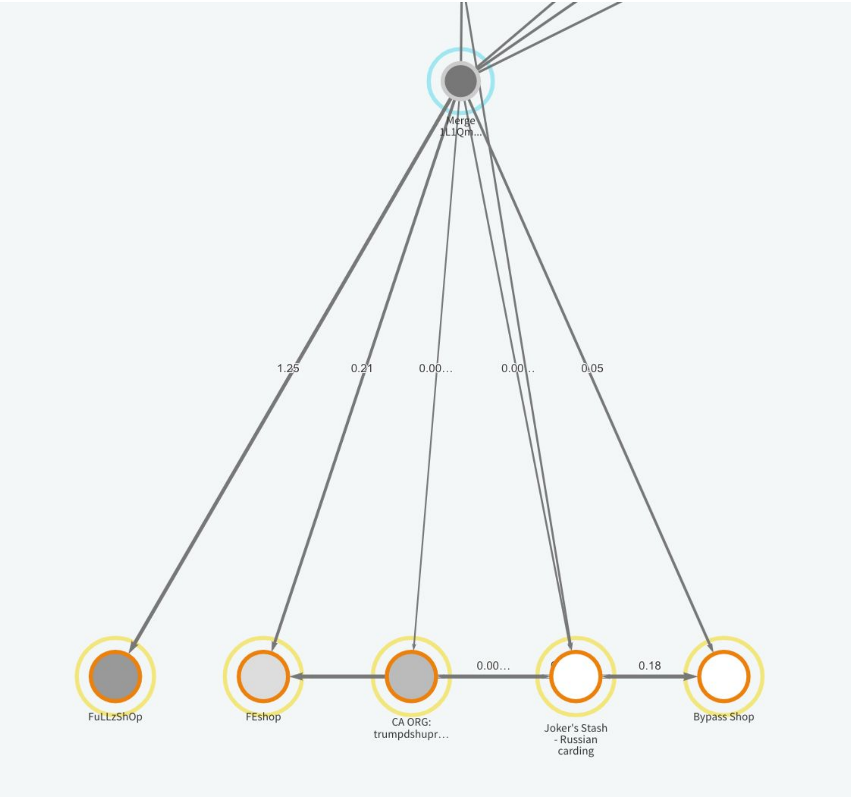


Traced	39,347,992.60 USD
Transfers received	3,776
Date Range	24/11/2017 - 05/06/2021



- All deposit addresses combined to one cluster
- Total value received is $39.3 million
- This may indicate links to other fraudulent activity
- Also received 41 BTC from Exchange 1 which may indicate other "mules" yet to be identified

The data: Links to other fraudulent activity



- When looking at the infrastructure of the OCG there is direct sending exposure to 5 prominent “Fraud shops”
- Around 1.5 BTC has been sent to these online marketplaces - aprox €80k
- Personal data / credit card details being purchased to facilitate other forms of fraudulent activity

Key Takeaways

- Opportunistic and very simple fraud to implement.
- Low risk high reward
- Fraud does not generate overt indications or exposure to “illicit” activity. Exchanges are unaware of the fraudulent origin of these funds.
- Undoubtedly links to other fraud campaigns - maybe yet to be reported or identified
- OCG network can be mapped out
- Substantial asset recovery totals available - “pay for itself” - reinvest in training & capabilities
- Public / Private collaboration is key
- Increased actionable intelligence - disseminated to other LEAs
- A clear MO has been identified - this can be shared for the benefit of other agencies