AASG
Accountancy AML Supervisors' Group

Fraud and Cashing Out Mechanisms

Extract from updated NCA Amber ALERT of August 2022 (Reference 0702-NECC)

Overview

This is a summary of a JMLIT+ Amber Alert is issued by the Fraud Cashing-Out Mechanisms Public-Private Threat Cell ("the Cell"), commissioned under the JMLIT+ Money Laundering Public-Private Threat Group.

The purpose of the alert is to provide a structural typology to the priority mechanisms through which fraud proceeds of crime are "cashed out". Cashing out is defined for the purpose of this Alert as being successfully realised and includes, but is not limited to, the operation of networks of mule accounts.

This alert should be read in conjunction with the AASG Alert (0701-NECC) on Fraud and Money Mules.

Information Report

Members of the Cell conducted strategic analysis of cashing-out destinations of suspected fraud funds and the key findings are summarised below:

1. Electronic bank transfers are almost certain to be critical to the operation of fraud laundering networks at scale.
2. Crypto-asset exchanges, Money Service Businesses (MSBs) and Payment Service Providers (PSPs) are highly likely to make up a major prevalent mechanism within the later stage layering and cashing-out process for fraud funds.
3. It is likely that crypto-exchanges, MSBs and PSPs are used to transfer value between jurisdictions for organised crime networks (OCNs) and individual offenders outside the UK that are targeting victims both in the UK and in third countries.
4. Cash withdrawals via ATM and branch are highly likely to make up a small proportion of cashing-out proceeds. It is likely that these cash withdrawals represent the 'incentivisation' fee for money mules.
5. Card payments are likely to make up a moderate proportion of fraud funds laundering by volume of transactions, but a lower proportion by scale.

The Cell's work gives preliminary insights into the complex journeys of fraud funds as they head towards "cashing-out". As with many money laundering techniques, illicit funds are often mixed with legitimate funds. Therefore, accurately and definitively tracing 'pure' fraud proceeds as they travel through multiple accounts, (usually mule accounts), becomes highly challenging on a system level.

This analysis is intended to assist financial institutions, crypto-exchanges and other firms in the financial sector to understand the nature of transactions which relate to the movement and realisation of the proceeds of fraud. Identifying the points at which criminals "cashout" their proceeds of fraud can help law enforcement target offenders higher up the chain.

It also gives visibility of how offenders are abusing the financial system to move money, including weak points in the control framework that criminals will adopt on an iterative basis. This may assist those in the financial services industry in setting up and reviewing their internal controls.

Methodology

Three retail banking participants in the Cell ran this analysis. The participants used distinct collection parameters:

- Participant 1 (P1) identified a total value of GBP 65.8 million debits in 3,789 transactions over a five-month period, representing an average of GBP 16,864 per single transaction.

- Participant 2 (P2) identified a total value of GBP 15.8 million in 66,256 transactions over a 12-month period, representing an average of GBP 238 per single transaction.

- Participant 3 (P3) identified a total value of GBP 34.5 million in 6,803 transactions over a six-month period, representing an average of GBP 5,069 per single transaction.

The cause of the wide difference in transaction value is likely the result of some slight variations in approach. P1 and P3 applied a filter to only analyse debits at over 10% of the alerting amount, with a minimum value of GBP 250. The main result of this was to exclude small card payments for everyday living expenses, which otherwise make up a major proportion of the transaction volumes (but a lower proportion of transaction value) seen by P2, who did not filter out any of the debit activity over a 12-month period.

The Cell participants used a commonly-used fraud control tool powered by machine learning across the faster payments system to identify mule accounts within their institutions over a time-bound period. After these accounts were identified, the Cell participants ran analysis on debits by those accounts in order to understand where fraud proceeds are moving at scale.

Transaction Destinations

Some variations in the participants' interrogation of the data and their analytical outputs make granular comparisons less accurate and reliable, so these have not been included here. However, some useful high-level observations can be drawn out from the results shared by the participants.

The findings have been sanitised to avoid naming specific destination institutions.

Bank Transfer Analysis

Analysis of bank transfer data by the three participants, particularly according to the volume of payments received highlighted how:

- Crypto-asset exchanges featured heavily in aggregated 'top' recipients. For two participants, they comprised just under half of the top recipient list in terms of payment volumes.
- MSBs were also key recipients in one participant' s analysis, comprising nearly half of their top 20 recipient list.
- Other recipient types, including individuals, retailers and HMRC, did not suggest any kind of trend or pattern and would require further research to determine their relevance and significance.
- FinTech firms featured widely across all three participants in terms of the top sort codes in receipt of funds. They made up half or more of their respective top 20 lists when ordered by payment volumes.

Merchant Payments

Analysis of merchant payments by both volume and value of payments revealed:

- A high level of MSB payments. In one participant' s top 10 list they feature on four occasions, in another participant's list they appear seven times.
- Foreign exchange-related merchant payments also featured in two participants' lists.
- Cryptocurrency firms also appeared but to a much lesser extent when compared to the bank transfer analysis.
- Gambling-related merchants featured once on one participant's top 10 list and twice on another participant's list.
- Other merchant types included various well-known retailers, however as with bank transfers, there is no immediate trend or significance to these and further research would be required to determine their relevance and significance.

Cash Withdrawals

According to analysis made available by two participants, cash withdrawals were mostly made via ATMs, although branch counter withdrawals were a significant proportion. For P1, branch counter withdrawals were 34 per cent of volume and 76 per cent of value for cash withdrawals, whereas for P3 they were 14 per cent of volume and 23 per cent of value. Withdrawals via the Post Office were very low.

Review of Fraud Funds Layering through Crypto-assets

Section 7 Crime and Courts Act 2013 Intelligence Sharing Exercise

As a test case, two Cell members conducted analysis on GBP deposits (valued in tens of thousands) of fraud proceeds transferred from a suspected money mule consolidation account with a retail bank to a

cryptocurrency exchange. The retail bank participant disclosed this intelligence to a crypto-exchange Cell participant via the National Crime Agency, using the Section 7 Crime and Courts Act 2013 gateway.

The GBP was deposited in amounts below GBP 1000, in what was likely an attempt to avoid Anti-Money Laundering (AML) controls. The GBP deposits were converted into cryptocurrency and then transferred onwards. This can be considered as secondary placement and layering as opposed to pure 'cash-out'.

Cryptocurrencies have advantages over fiat in that every transaction is completed on an immutable blockchain and recorded on a public ledger. This allows for the completion of track and trace analysis by those who have the relevant skills and technically capability. This includes the use of blockchain forensic tools which assist in the identification and attribution of associated addresses and wallets.

In this case, Bitcoin (BTC) was the primary cryptocurrency for which the GBP was exchanged. Within the analysis, a proportion of the BTC was sent directly to a centralised exchanged (1st hop) and deposited into additional accounts. These accounts showed either the BTC being converted back into fiat (GBP) and withdrawn or being moved onwards again (moved off platform).

The wider track and trace analysis demonstrated interaction (2nd and 3rd hop) with centralised exchanges, which included the identification of common deposit addresses, suggesting coordination, along with the use of P2P exchanges and mixing services. The purpose of a mixer is to obfuscate the source of funds by severing the link between the "incoming" and "outgoing" funds.

This intelligence sharing exercise allowed a 'deep-dive' into one specific case. It supports the hypothesis that cryptocurrency is highly likely to be used as part of the 'cashing-out' layering process, but that ultimately the funds are still highly likely to make their way back to fiat for realisation.

Crypto Conclusions

There are two basic typologies to the laundering of fraud proceeds through crypto-assets. Increasingly, victims are deceived into paying fraud proceeds directly into crypto-wallets. These were not assessed by the Cell. Alternately, fraud proceeds are layered through fiat accounts before they are transferred into crypto-assets.

A major limitation identified by the Cell is that not enough is known about fraud funds re-entering the fiat system from the crypto-assets, as another stage on the laundering journey. As such, it is a realistic possibility that when a customer receives funds into their fiat bank account from a crypto-platform and the origin of these funds is unknown or unclear, they could be the proceeds of fraud.

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference **0701-NECC** within the text. This reference is specific to the Alerts process; where appropriate, we would ask that this is used in addition to the ongoing use of the Glossary of Terms. Guidance on making suspicious activity reports is available at www.nationalcrimeagency.gov.uk.

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer

The Accountancy AML Supervisors' Group (AASG) accepts no responsibility for any loss, damage or expense arising in connection with the use of information in this alert. Any use will be taken to signify agreement to these conditions.