AASG
Accountancy AML Supervisors' Group

Fraud and Money Mules

Extract from updated NCA Amber ALERT of August 2022 (Reference 0701-NECC)

Overview

This alert raises awareness of indicators of behaviours associated with Mule Accounts and links to fraud and money laundering. A key mechanism to cash-out the proceeds of fraud against individuals, the public sector and private sector is the use of mule accounts.[1]

This alert should be read in conjunction with the AASG Alert (0702-NECC) on Fraud Cashing-Out Mechanisms.

Mule Accounts Overview

Mule accounts are widely used to facilitate both low-tech cyber enabled fraud attacks such as authorised push payment, as well as in high-tech cyber dependent attacks involving malware. They are also used to deposit street cash into the banking system and in variations relating to the purchase of high-value goods and crypto-assets in order to transmit value.

Mule accounts are defined as intermediary accounts used for money laundering, acting to create complex transaction chains in order to reduce detection by the financial services sector and law enforcement of an Organised Crime Network (OCN) and/or individual offenders.

Mule accounts might be operated by a money mule, which is a person who transfers illegally acquired money on behalf of others knowingly or unknowingly. Often, however, a mule account is controlled by a recruiter (sometimes known as a herder), potentially on a temporary basis, after the account holder has provided the recruiter with their account details, bank card, pin and/or passwords in exchange for a fee.

Mule accounts can also be acquired through victimisation and exploitation of vulnerable persons.[2] Mule accounts can be opened and operated by criminals who commit fraud using false representation, without the knowledge of the natural person named as the account holder.

Mules are at the bottom of the hierarchy of a criminal network. Lower-tech fraud networks are more likely to recruit locally through personal or social networks, with the key audience profiles for mule recruitment being under 30s and students (although not limited to these categories). Higher-tech networks are more likely to recruit online, e.g. using spurious job adverts, and acquire mule accounts across different jurisdictions.[3]

Mule Account Holder Profiles

Mule account holders largely fall into one of three involvement categories:

1. **Witting**
    - **Complicit:** Account holder is a complicit money mule, aware of the criminal source of funds, acting through their own choice and typically motivated by a financial incentive. The mule is likely to be directly involved in person in-cash transactions into or out of their account and may become involved in recruiting others.
    - **Negligent/Naïve:** Account holder should reasonably have had some suspicion, for example, after receiving no assurances or credible cover stories from their recruiter regarding the source of funds. However, they have insufficient information about the original crime ("predicate offence") or full knowledge of the criminal nature of the work to

[1] For the purposes of this Alert, 'mule account' should be considered to include hosted wallets with a regulated cryptocurrency exchange and a payment service provider.
[2] Definitions of vulnerability exist in law. For example, the Modern Slavery Act 2015 refers to a person's personal circumstances – such as the person being a child, their family relationships and any mental or physical illness.
[3] Rutger Leukfeldt & Jurjen Jansen, "Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands"; International Journal of Cyber Criminology, p.182

be considered complicit in a money laundering offence. They may have potentially handed over their bank card and pin to a recruiter.

2. **Unwitting (Victim)**
    - **"Active" Victim of Fraud:** Actively engages in mule activity albeit under fraudulent, non-employment pretences. The mule may be a victim of crime themselves, such as a romance fraud victim.
    - **Unwilling:** Mules engage in activity due to vulnerability or under coercion. The mule may be vulnerable, for example, abuse of indebted drugs mules in County Lines.[4]

3. **Unknowing (Victim)**
    - **"Inactive" Victim of Fraud:** Account is acquired and used without the knowledge of the account owner. The account holder may be a victim of identity theft or may be impersonated by criminals.
    - **Fake Accounts:** Accounts created wholly using fraudulent documents, for example it may be created using false identification.

Cash Deposits

Mule accounts may be used to divide large transactions into smaller increments, sometimes known as smurfing or structuring. Smurfing can involve depositing cash proceeds into the banking system as a stage in the layering process in order to distance the criminal funds from the original (or "predicate") offence.

These cash deposits are frequently used to launder physical cash generated by the trafficking of illegal drugs, as well as through tax fraud, notably alcohol and cigarette duty evasion and Value Added Tax (VAT) fraud, all of which can generate significant volumes of street cash.

Cash couriers[5] are excluded for the purposes of money mule activity where there is not a cash deposit into the financial sector.

Mule Account Indicators

The following typologies outline different types of money mule accounts, which are drawn from case studies. It is worth noting that OCNs and offenders are highly likely to use a combination of different methods to obtain as many mule accounts under their control as possible.

This list is not definitive and there will be crossovers between different types of mule accounts. Criminals will be dynamic in their deployment and development of new methods.

Mule Account Type	Typical Predicate Offence	Indicators
WITTING		
Cash depositor	Professional money laundering for commodity Organised Crime Groups (OCGs) (drugs, excise fraud, organised immigration crime)	• Significant branch or Post Office cash deposits without legitimate explanation • Same day / closely-spaced cash deposits across multiple branches or regions • Deposit values below arbitrary round numbers (e.g. GBP 10,000) • Indicators of East Asian Underground Banking9 and/or Informal Value Transfer System10 / Hawala11 banking • Purchase of significant volumes of high-value luxury goods (also see " Daigou" type below) • High concentrations of Scottish and Norther Irish banknotes

[4] County Lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs into one or more importing areas [within the UK], using a dedicated mobile phone line or other form of 'deal line'. They are likely to exploit children and vulnerable adults to move [and store] the drugs and money and they will often use coercion, intimidation, violence (including sexual violence) and firearms.

[5] Cash couriers are individuals who physically transport currency on their person or accompanying luggage, usually from one jurisdiction to another.

Local recruit (witting)	Low-tech cyber enabled fraud such as APP, Self-Assessment fraud, DWP fraud	• Account / wallet holder recruited online (Instagram, Snapchat and Telegram are most common, but Facebook and other encrypted messaging apps may also be used) and / or face-to-face • Recruitment under no or very limited false pretences, frequently targeting students and quick-cash opportunists • Account holder may provide bank card and PIN / password to recruiter, in exchange for a fee (typically a percentage of fraud funds) or other benefit (e.g. luxury goods) • Test payments (also known as " coupling") to make small payments to link accounts together to legitimise new payees and IP addresses • Suspicious activity continues despite being contacted by financial firm
Mules-as-a-service	Fraud and cybercrime (both enabled and dependent), such as advanced fee / cloned website, impersonation fraud	• Account holders are natural persons overseas recruited through online forums and/or Telegram channels, and opening accounts online through overseas IP addresses (often in the former Soviet Union) masked through high-risk VPN providers • Account openings targeted at FinTech12 firms or gambling companies that allow online electronic verification • Account opening videos show Cyrillic script on road signs or clothing • Transactions to/from crypto-currency exchanges • Transactions to/from payment service providers (PSPs) / electronic money institutes (EMIs)
Consolidation account	Fraud against individuals, the private sector and the public sector	• Merging point for multiple fraud / other criminal payments, potentially at fourth or fifth generation of fraud funds (or more)13 • Transactions to/from crypto-currency exchanges and wallets • For cryptocurrency wallets, funds may re-merge after they have been through a tumbler service • Transactions to/from payment service providers (PSPs) / electronic money institutions (EMIs) • More likely to be a business bank account **For company accounts:** • Linked with a UK company newly registered with Companies House or purchased ' off-the-shelf ' from a formation agent • May be used to co-mingle funds from multiple crime types alongside legitimate income • May have been used for Bounce Back Loan frauds

Daigou shopper[6]	Professional money laundering for commodity OCGs (drugs, excise fraud, organised immigration crime) VAT fraud on export of luxury goods (typically by the company "employing" the shopper)	**For retail banking:** • Significant cash deposits or transfers from another account in receipt of cash deposits, followed by a bulk shopping spree on luxury goods • Use of second personal account in order to keep activity from impacting on their primary account • Frequent payments from the Daigou company bank account to employees (on PAYE and subcontractors) that do not fit with a regular salary • Shoppers paid a minimum wage, sometimes as low as GBP 5,000 per annum PAYE, and generally under GBP 25,000 per person • Frequent payments from the employee to the Daigou company employer • Account turnover may be in the tens or hundreds of thousands of pounds, with a Daigou shopper receiving funds to purchase Daigou goods and refunding unspent amounts to the company • Daigou Company " employees" (on PAYE and subcontractors), who themselves are directors of companies • Transfers into the company account(s) and/or Director(s) personal account(s) from personal / student bank account **For credit card companies:** • Shoppers are made additional users on company charge card accounts, balances of which are usually settled by the company • Bulk purchase of " Daigou goods" , typically luxury goods • Thousands of pounds being spent at the same retailer or within short periods of time with repeat purchases of the same amounts, indicating purchase of duplicate goods • Daigou Company " employees" (on PAYE and subcontractors), who themselves are directors of companies. • Significant volume (sometimes thousands of pounds) of purchases of goods using multiple gift, charge or credit cards. • Supplementary users added to Directors' personal cards, with balances settled by the company, not the user of the cards.
NEGLIGENT		
Sold account	Coronavirus support scheme fraud Low-tech cyber-enabled fraud attacks, such as APP	• Original account holder has sold on account and password to money launderer after leaving the country, for example an overseas student after they finish their studies • Criminal/launderer changes passwords and establishes new online

[6] For more information, refer to JMLIT Alert 0624-NECC Daigou Tax Evasion Typologies

		banking access under their own control (masked through multiple devices and/or other operational security) • Test payments (also known as " coupling ") involving small payments to link accounts together to legitimize new payees and IP addresses • Account details provided to impersonation fraud victim as a " safe account" for the victim to pay funds into.
Local recruit (negligent)	Low-tech fraud attacks, such as APP, DWP fraud, Self-Assessment fraud	• Account holder recruited online (Instagram, Snapchat and Telegram are most common, but Facebook and other encrypted messaging apps may also be used) or face-to-face • Recruitment under limited false pretences • Low value / quantity of fraud transactions received into account • Stops when notified by financial firm
Scam victim	Fraud against individuals, the private sector and the public sector	• Person recruited through fake job advert or other social engineering, and convinced by assurances of legitimacy • Account is compromised by criminals with the aim of deceiving the account holder's friends into providing their bank or PayPal details • Stops when first notified by financial firm
UNWITTING		
False representation	Fraud against individuals, the private sector and the public sector High-tech cyber dependent attack (malware)	• Account opened through false representation, with the offenders, not the named account holder, in control of the account. • Types of document used to pass KYC checks may include:[7] ○ Fraudulently obtained genuine (FOG) documents – documents issued authentically but applied for using false information ○ Counterfeit documents - A reproduction from scratch of an officially issued document ○ Forged documents – A genuine document altered in some way, such as with changed personal details (often a utility bill or bank statement) ○ Pseudo documents – Documents with the appearance of a legitimate document, but which are not officially recognised ○ Impersonation documents – person is a " look-alike " presenting someone else ' s genuine documents

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869551/Guidance_on_examining_identity_documents_v._February_2020.pdf

		• Such account openings may involve the use of stolen personally identifiable information (PII), such as purchased through the dark web • Forged utility bills are frequently used for address verification • Dense clusters of such accounts using a single address suggests the OCN / offender has connection with a natural person at that address or mail forwarding in place • Likely crossover with " mules-as-a-service" above
Vulnerable person	Modern Slavery, Human Trafficking and Organised Immigration Crime offences	• Account holder is a person who for physical or health reasons can reasonably not be expected to manage their finances • Potential victim of trafficking, for example debt bondage, adult sexual exploitation and/or coerced criminality • Significant physical or mental health illness (major disability, dementia etc.) • Person suffering from serious addiction (illegal drugs, alcohol, gambling) • Children (i.e. any person under 18) • Person (typically a woman) in a coercive or abusive familial or intimate relationship
Social engineering victim	Romance fraud, Business Email Compromise fraud	• If older and female, they are more likely to be a romance fraud victim, where the account is repurposed after it has been emptied and the account holder is deluded into believing they are in a romantic relationship • If younger and male, potential to be sextortion victim blackmailed into moving money (e.g. after soliciting of intimate images under false pretences)

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.