Australian Government
AUSTRAC

Fintel Alliance
An AUSTRAC initiative

AFP

Australian BORDER FORCE

COMBATING THE EXPLOITATION OF

INTERNATIONAL STUDENTS AS MONEY MULES

FINANCIAL CRIME GUIDE JUNE 2024

COPYRIGHT

ATTRIBUTION

ACKNOWLEDGMENTS

This financial crime guide was developed by Fintel Alliance, a public-private partnership led by AUSTRAC.

Thank you to all of our partners who contributed to this financial crime guide.

CONTENTS

HOW TO USE THIS FINANCIAL CRIME GUIDE

This financial crime guide has been developed to assist government agencies and financial service providers, including remittance service providers and digital currency exchanges, to understand and identify signs of criminal networks exploiting vulnerable members of the community as money mules.

The indicators and behaviours in this financial crime guide can be used by financial service providers to review their profiling and transaction monitoring programs to target, identify and stop financial transactions associated with money mule activity.

It can be difficult to detect individuals at risk of becoming money mules, or those ultimately controlling the illicit funds. No single financial indicator will definitively identify if an account is being used for money mule purposes. Financial service providers should use a combination of indicators highlighted in this guide and business knowledge to conduct further monitoring and identify if there are reasonable grounds to submit a suspicious matter report (SMR) to AUSTRAC.

SUSPICIOUS MATTER REPORTING

If you identify possible indicators of money mule activity or other criminal activity through financial transactions and determine you need to submit an SMR, include clear behavioural and financial indicators in your report. This will help AUSTRAC and our law enforcement partners to respond and take action.

For more information, see the various available resources[1] regarding effective suspicious matter reporting on the AUSTRAC website.

ABOUT FINANCIAL CRIME GUIDES

Financial crime guides provide detailed information about the financial aspects of different crime types. They include case studies and indicators that can be used to identify if a potential offence is occurring.

They are developed with AUSTRAC's Fintel Alliance partners, relevant government agencies and industry partners. This guide was developed by Fintel Alliance in partnership with the Australian Federal Police (AFP) and Australian Border Force (ABF).

1 austrac.gov.au/business/core-guidance/reporting/suspicious-matter-reports-smrs

ABOUT FINTEL ALLIANCE

Fintel Alliance is a public-private partnership led by AUSTRAC that brings together government, law enforcement, private sector and academic organisations who work together to:

- support law enforcement investigations into serious crime and national security matters
- increase the resilience of the financial sector to prevent criminal exploitation
- protect the community from criminal exploitation.

Fintel Alliance partners include businesses from the financial services, remittance and gaming industries as well as law enforcement and security agencies in Australia and overseas.

THE IMPORTANCE OF PARTNERSHIPS

Fintel Alliance's public-private partnership is an effective way to identify the roles and activities of criminals involved in money mule activity. Partners work together to develop shared intelligence and deliver innovative solutions to support financial service providers to detect, disrupt and prevent this crime.

INTRODUCTION

A criminal network consists of a connection of relationships between individuals and/or organised crime groups, including money laundering organisations[2] who engage in illicit activities for financial gain.

Criminal networks involved in a wide range of crime types including human trafficking, drug trafficking, scams and fraud, seek to launder their illicit funds and reintegrate their profits back into the economy. Whether it is to increase wealth, reinvest in further offending or avoid seizure, criminals need to move money.

One of the ways that criminal networks launder illicit funds is through the use of money mules, which creates distance between the networks and the crime, and helps to avoid detection by law enforcement. Criminal networks seek to exploit vulnerable members of the community to act as money mules to move the proceeds of crime for them. They often target international students and non-permanent residents, offering them a way to make money while living in Australia.

ABOUT MONEY MULES

A money mule is someone who transfers or moves illegally-acquired money on behalf of someone else. Money mules can move funds in various ways, whether it be physical cash, through bank account transfers, obtaining and depositing cashier's cheques, digital currency, use of prepaid debit cards, or via remittance service providers. Money mules may move money using a personal or company bank account, someone else's account, or may be instructed to register a company and then open a business bank account.

Different money mules can be involved in separate phases of the laundering process and may be unaware of the existence of others and their roles. At times, mules may voluntarily provide assistance to criminal networks. For instance, they may respond to advertisements looking to purchase personal bank account details once they are no longer needed, and sell their accounts to criminal groups for mule activity. However, some money mules are unaware that their actions are illegal, often believing their facilitation of funds transfers relates to legitimate employment. This makes it incredibly important for members of the public to protect themselves from becoming a money mule. They should be vigilant of any red flags and report suspicious requests or activity to local law enforcement.

WHY THE TERM 'MONEY MULE'

The term 'mule' originates from an animal crossed between a horse and donkey typically used to carry the load for others. Money mules are used to carry the risk involved with laundering illicit funds. Criminal networks will use a money mule, their identification and/or their account details to distance themselves from these illicit funds.

2 A money laundering organisation (MLO) is an organised criminal network which specialises in laundering the proceeds of crime. They are professional money launderers with international reach. These MLO networks are hierarchical and consist of defined roles, including the role of money mules.

RECRUITMENT OF MONEY MULES

The AFP, AUSTRAC and ABF have identified international students and non-permanent residents in Australia as high-risk groups who are vulnerable to being recruited as money mules.

- International students currently studying in Australia can be recruited as money mules in order to earn money while studying.
- Other money mules are sent to Australia by criminal networks and exploit student visas as a means of entering the country to conduct money mule activity, with no genuine intention of studying.

Criminal networks use a variety of means to recruit foreign student money mules through face-to-face contact or online platforms. They target both legitimate and illegitimate student visa holders and can recruit others outside of the student cohort.

TRUSTED INSIDERS

Foreign student money mules can be targeted for recruitment by trusted insiders. A trusted insider is anyone with access to a business's systems, either in Australia or overseas. An example of a trusted insider is a complicit migration agent or person used to assist with visa applications, the provision of education or relocation requirements. These people are in daily contact with students and are trusted with personal details that can be used by criminal networks for recruitment purposes.

ONLINE PLATFORMS

Foreign student money mules can be recruited online through means such as online gaming platforms, social media, chat forums and online advertisements. Recruiting individuals online assists in keeping the identity of criminals hidden and unidentifiable by the money mule if they are detected by law enforcement. Regardless of how they are lured, individuals are offered payment in exchange for opening accounts and registering companies in their names, which are then used to launder funds by criminal networks.

LEGITIMATE VISA HOLDERS

Criminal networks are targeting legitimate visa holders as they are leaving Australia including students who have completed their studies and individuals on temporary visas that are yet to expire. These individuals are paid by criminal networks who purchase existing account and identification details no longer needed by the departing individual. These accounts and identification details are then used to open additional bank accounts and launder illicit funds.

ILLEGITIMATE VISA HOLDERS

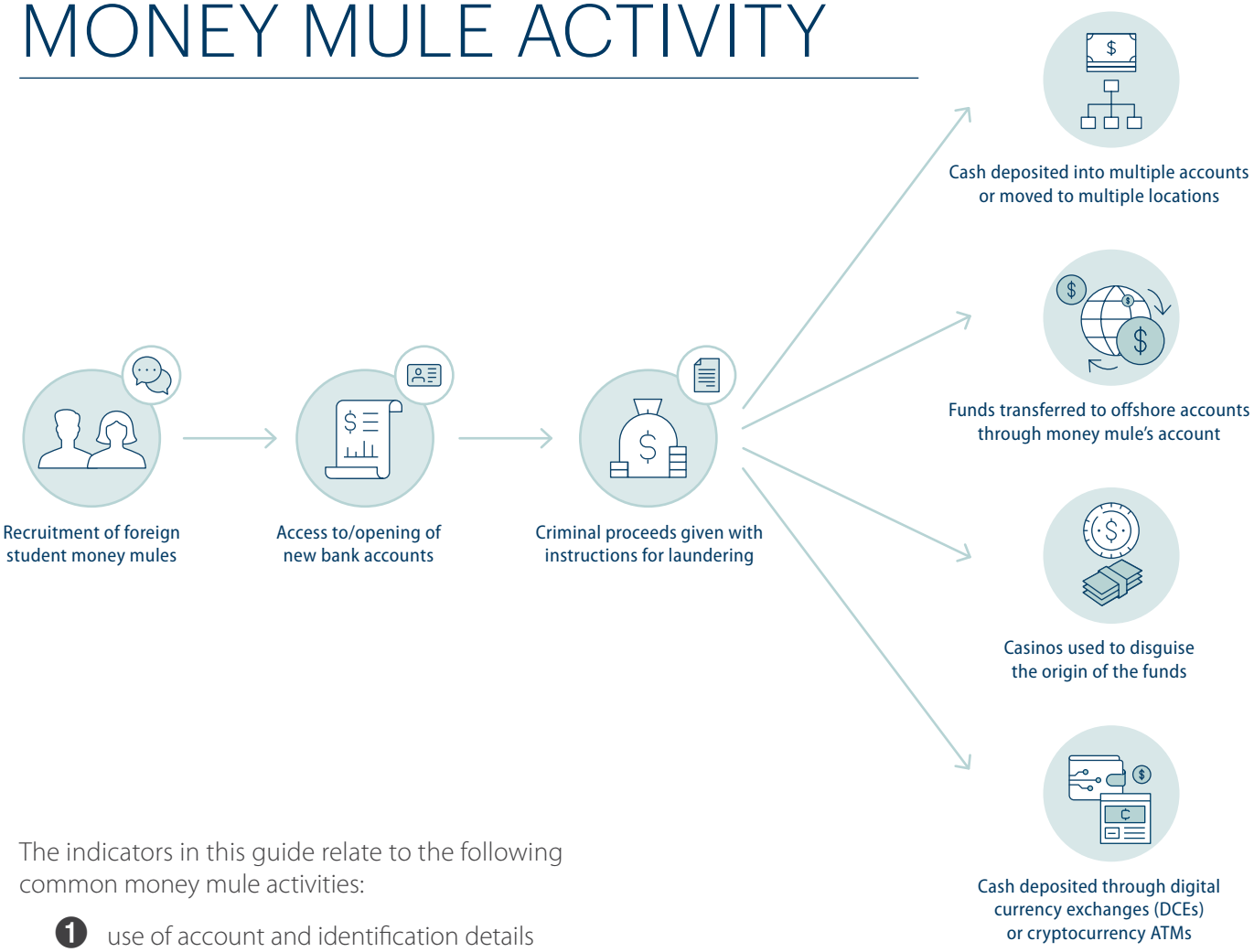
Upon instruction by criminal networks, some internationally-based individuals acquire visas as a guise to travel to Australia before engaging in money mule activity. These individuals have no intention of studying and shortly after arriving will create bank accounts and establish identification documents that are then passed onto the criminal network. These individuals then leave Australia, and their accounts and identification are used to launder illicit funds.

STUDENT VISAS

Australian visa subclass 500 allows the holder to stay in Australia for the purposes of study for up to five years. This visa allows holders to work up to 48 hours a fortnight. Students must be six years or older and enrolled in a course of study in Australia.

INDICATORS OF

MONEY MULE ACTIVITY



The indicators in this guide relate to the following common money mule activities:

1. use of account and identification details
2. identification details used to register companies
3. cash couriers
4. fraud and scam-related mule activity
5. casino money mules
6. cryptocurrency money mules.

These indicators have been drawn from known case studies and existing indicators of money mule activity seen in financial services reporting.

The indicators should be considered as part of a risk-based approach in transaction-monitoring programs, investigations and/or due diligence processes. Financial service providers should use a combination of customer and financial indicators, combined with knowledge of their business to monitor, mitigate and manage risks associated with any unusual activity.

Where a suspicion is formed, financial service providers must give consideration to their SMR obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

NOTE: Although these indicators have been drawn from international student money mules, many will be relevant to other money mule categories.

❶ USE OF ACCOUNT AND IDENTIFICATION DETAILS

Criminal networks often purchase bank accounts and identification details from foreign students who are either finalising their study and about to leave Australia, or as a means for them to earn money while in Australia. Criminal networks then use these accounts and identities to launder funds and create new banking customer profiles and accounts across multiple financial institutions.

These accounts are critical in the placement and layering stages of the money laundering cycle and enable:

- circumventing daily banking limits of individual accounts
- increased volume of funds to be moved
- increased number of bank accounts controlled by the criminal network
- reduced know your customer (KYC) requirements for profiles that are already established.

In cases where accounts have been purchased from students permanently departing Australia, the account activity may initially appear typical of a student. Purchases for plane tickets and travel-related expenses may be seen before activity temporarily ceases, indicating the individual has departed Australia. Shortly after, online banking profiles are used by the network to open new accounts, indicating they are under the control of the criminal network.

Individuals who become money mules on first arriving in Australia will have significant funds flowing through their accounts shortly after arriving. These individuals have no declared income, and the funds received are disproportionate to their profile and unable to be accounted for by educational or familial support. Activity like this could indicate the account holder is acting as a money mule or that the account is controlled by a criminal network.

Multiple individuals recorded at the same residential, IP and email address and/or against a common phone number are indicators that a third party is using someone else's identification details to open accounts for mule activity.

SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

- Students and non-permanent residents from East Asia are higher risk but this is not an exclusive indicator.
- Individuals with international passports and/or proof of age cards and who identify as a student.
- Targeted by online games and advertisements.
- Targeted by migration agents and/or international student support organisations.
- Targeted when they first arrive in Australia or as they are departing Australia.

FINANCIAL INDICATORS

- Significant funds flowing through accounts shortly after arriving in Australia.
- No declared income.
- Disproportionate amounts of funds through accounts that cannot be accounted for by income or familial/educational support.
- Multiple accounts and/or profiles opened across one or multiple financial institutions.
- Common residential addresses, IP addresses, email addresses and/or phone numbers recorded against multiple customer profiles.
- Plane ticket purchases and several travel-related expenses recorded. Shortly after, online banking profiles are used to open new bank accounts.

❷ IDENTIFICATION DETAILS USED TO REGISTER COMPANIES

Foreign student money mules have been identified registering companies and becoming directors for the purpose of establishing a front to launder illicit funds. These companies are used to create company accounts with financial institutions. Criminal networks can draw from a pool of these 'shell companies' to move money themselves or by instructing the director, known as a 'dummy' or 'straw' director to do so.

These companies may:

- have no online presence
- have very few business-related transactions (i.e. payroll, tax, everyday business expenses) associated with their accounts
- receive high-value or volume government payments inconsistent with their customer profile
- be registered to a residential address
- have related company profiles that can be identified through common addresses and similarly structured business names, and may relate to cash-intensive industries like building and construction
- be registered by individuals on a student visa who have recently arrived in or departed from Australia
- be directed by a student or non-permanent resident but controlled by a third party (i.e. someone else is the account signatory)
- have transactions that are inconsistent with their stated industry

SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

- Company directors or secretaries are individuals on student visas who have recently arrived or departed Australia.

FINANCIAL INDICATORS

- Companies displaying limited business-related transactions.
- Companies receiving significant government payments inconsistent with their profile.
- Company address is residential.
- Multiple companies with a common registered address and similarly structured names.

❸ CASH COURIERS

Cash couriers are a type of money mule used to physically move cash by taking on a contract for 'cash runs'. A cash run is conducted by an individual who transports cash or makes cash deposits into multiple accounts at multiple locations, as instructed by a criminal network, over a concentrated period of time. These cash runs are usually done over a few days with the intention to place the funds into the financial system quickly (a two-week run is considered long). Some cash run contracts run for two to three days per month on a regular basis.

Cash couriers are used as conduits for criminal networks to distance themselves from the risks of moving cash, and they earn money for their services. These networks attempt to make it more difficult for their activity to be detected by using multiple accounts across different financial institutions and locations.

To avoid drawing unwanted attention, cash couriers will commonly use nondescript or unassuming bags such as supermarket and cooler bags to transport the cash to be deposited, carrying up to $500,000 per bag. Identifying the individuals making account deposits is important as they may have more significant involvement in the organised crime group.

Cash couriers may have also purchased or be in possession of:

- bank cards
- bank receipts
- proof of identity
- ledgers
- bank notes
- cash counting machines
- several mobile phones
- freezer bags, supermarket shopping bags, cooler bags
- elastic bands.

SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

In possession of items such as:

- supermarket shopping bags
- freezer bags
- cooler bags
- elastic bands
- bank cards and receipts
- copies of or written identification details
- ledgers
- cash counting machines
- mobile phones.

FINANCIAL INDICATORS

- Cash runs – cash deposits into different accounts over a concentrated period of time.
- A single depositor making deposits into multiple accounts.
- A single account receiving deposits from multiple depositors.
- concentrated deposits or withdrawals at the same branch, ATM, location or suburb.

CASE STUDY

A Melbourne woman was scammed out of nearly $300,000. A person falsely identifying themselves as a bank employee contacted the woman from an unlisted number and said they had identified suspicious transactions on her account. The woman gave the caller remote access to her online banking and security codes. Around $300,000 was then transferred out of her account to 11 money mule accounts, with the funds being withdrawn from ATMs soon after.

Most of the mule accounts belonged to Indian students who had set up the accounts with legitimate identification details. The students had returned to India at the time the money was withdrawn from their accounts, indicating someone other than the students had control of their accounts.

4 FRAUD AND SCAM-RELATED MULE ACTIVITY

Criminal networks use foreign student money mules to open Australian bank accounts and transfer funds offshore that were derived from scams, fraudulent loan applications and other types of fraud. These funds are often received by mules in cash before being deposited into the mules' accounts. Often money mules participating in this activity come to Australia under a foreign student visa, but do not attend or participate in any study while in Australia.

These money mules will often conduct regular ATM cash deposits before rapidly transferring the money to money remitters, digital currency exchanges and internationally, predominantly to South Asia. These transfers are disproportionately higher than expected wages for a student and are often made to countries inconsistent with the account holder's home country, or ethnic or cultural background. International transfers are sent during intense periods of account activity, with large amounts being consolidated and sent on the same day or during a short period of time. Low value 'test' transfers have also been identified, usually under $10.

Mules are paid anywhere between $200 to $500 for the use of their own accounts, and may receive about 10 per cent commission on funds received into nominal accounts they operate. Accounts opened using stolen, fraudulent or purchased identity documents are usually opened online at a single or multiple institutions over a one-to-four-day period, however this could be longer. In many instances common addresses, phone numbers and email addresses are used across multiple accounts, and linked to multiple identities.

Characteristics of fraud or scam-related student money mules include:

- typically male
- aged approximately 30 and under
- from South Asia
- a visa history that includes cancellations, breaches (including for overstaying) and/or multiple granted visas
- multiple educational course changes
- failure to attend their enrolled course, or are course non-compliant.

These mule accounts are often used to purchase high-cost items such as high-end phones or luxury clothing, despite account holders receiving limited financial assistance from their home countries. This spending pattern indicates a lack of intent for the student to actually study in Australia. Money mules (or those controlling their accounts and identities) on student visas may be applying for multiple credit cards and opening multiple accounts to facilitate money mule activity. Many record three or more Visa Entitlement Verification Online (VEVO) checks against their name by finance and insurance service providers.

SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

- Age 30 years old and under.
- From South Asia.
- Poor visa history.
- Do not end up studying in Australia.
- Multiple VEVO checks against name.

FINANCIAL INDICATORS

- International transfers to South Asia.
- Transfers to money remitters.
- Funds obtained are disproportionate to or inconsistent with a student's wage.
- Large amount of international transfers sent in short period of time.
- Low value 'test' remittances under $10.
- Multiple credit and debit accounts opened.
- Purchases of high-cost items such as high-end phones and luxury clothing.
- Lack of financial assistance from South Asia.

CASE STUDY

A Vietnamese-Australian organised crime figure known as 'aunty' was running a money laundering organisation, using student money mules to launder funds on behalf of organised crime groups.

Mules were used to deliver cash to the money laundering premises, which housed items including cash counting machines, mobile phones, freezer bags and elastic bands all used to handle the illicit cash.

❺ CASINO MONEY MULES

There are multiple ways foreign student money mules are being used to launder funds through casinos. This includes cash deposits and the purchase of 'casino value instruments' such as gaming chips, ticket-in ticket-out tickets, gaming machine credits and cashier's orders. The cash-intensive nature of casinos is appealing to criminal networks seeking to legitimise their illicit funds, although this has become somewhat limited in recent years due to internal controls being placed on the amount of cash individuals can use at some casinos.

Casino money mules have been found to take up to 10 per cent as a commission for laundering funds on behalf of criminals. Once the illicit funds have been placed and layered through a casino, mules may use a company or mule account to further disguise the source of the funds, and/or use unregistered and registered remittance providers to transfer the funds internationally.

The casino channels money mules may be exploiting include:

- purchasing casino chips with illicit funds to distance the origin and intended recipient
- transferring physical casino chips to patrons
- exchanging small denomination notes for larger denominations
- exchanging foreign currency to Australian currency with no gaming play
- obtaining casino disbursement cheques for winnings or non-winnings
- depositing higher values and/or larger volumes of cash at casinos to disguise the origin and ultimate recipient of the funds.

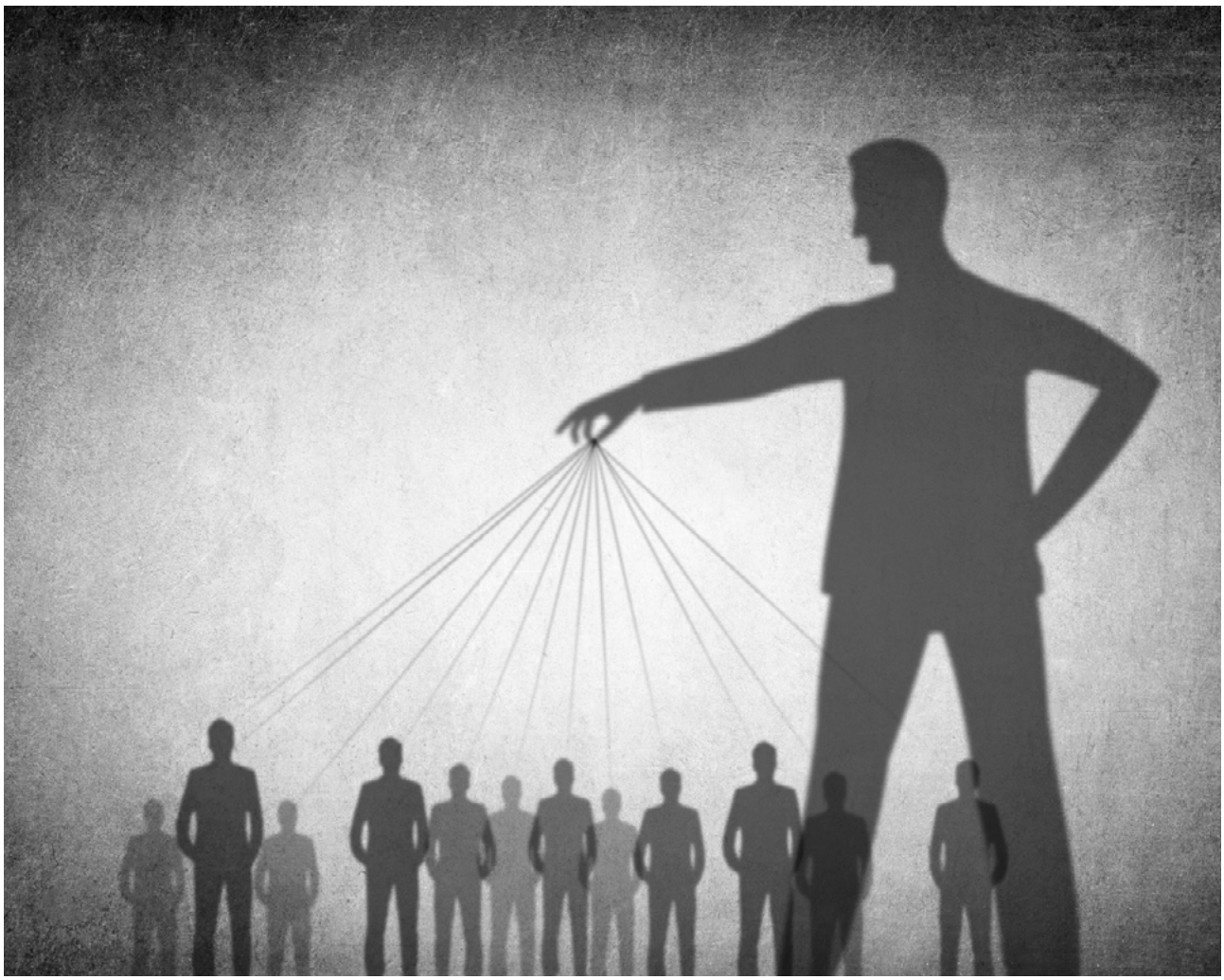
SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

- Age 30 years old and under.
- Students and non-permanent residents from East Asia are higher risk but this is not an exclusive indicator.
- Individuals with international passports and/or proof of age cards and who identify as a student.
- Directors or secretaries of recently incorporated companies.
- Has access to more cash or wealth than would be expected for customer profile.

FINANCIAL INDICATORS

- Chip purchases.
- Cash and bank draft deposits.
- Transferring chips.
- Exchanging small to large denomination notes.
- Obtaining casino disbursement cheques.
- Carrying large amounts of cash.
- Sending funds internationally using remittance networks.
- Earning a percentage as a commission.



❻ CRYPTOCURRENCY MONEY MULES

Foreign students are being used to deposit cash at digital currency exchanges (DCEs) and cryptocurrency ATMs. The money mules setting up these accounts often have little knowledge of cryptocurrency and may indicate they are transacting on behalf of someone else. Deposits are often made on sequential dates at similar times, with blockchain analysis identifying related payee addresses receiving deposited funds.

The mule accounts are often used to launder money in broader-networked activity across multiple account types, financial platforms and devices. The use of privacy or peer-to-peer wallets and tumblers or mixers is also common. Transactional activity within the network will typically have points of convergence such as multiple customers' withdrawal addresses transacting with each other on the blockchain; or the funds from seemingly unrelated mules being ultimately traced to the same offshore or high-risk DCE.

CASE STUDY

Young female international students were escorted by a male to deposit up to $100,000 cash per transaction. Four females in the group deposited a total of $1.4 million cash within a 21-day period. These students were of Southeast Asian ethnicity and were used on multiple occasions to deposit cash at DCEs.

SUMMARY OF INDICATORS

INDIVIDUAL INDICATORS

- Mostly females.
- 30 years old or younger.
- Southeast Asian ethnicity.
- No criminal history.
- Sometimes escorted by a male.

FINANCIAL INDICATORS

- Cash deposits up to $100,000 per transaction.
- Deposits made at DCEs and cryptocurrency ATMs.
- Cash deposits inconsistent with expected student income.
- Deposits made on sequential dates at similar times.
- Common digital currency payee addresses.

STOPPING MONEY MULE ACTIVITY

Criminal networks are recruiting foreign student money mules using multiple techniques that typically seek to exploit vulnerable members of the community. Once recruited, their activity is conducted using a variety of methodologies, platforms and financial sectors that continually evolve and adapt to evade detection. The above financial and individual indicators can help detect money mule activity and harden the financial sector to make this form of money laundering more difficult for criminals.

REPORTING SUSPICIOUS BEHAVIOUR

Observing one of these indicators may not suggest illegal activity on its own. When you conduct further monitoring and observe other activity that raises suspicion, you should submit a suspicious matter report (SMR) to AUSTRAC.

High-quality, accurate and timely SMRs give us the best chance to detect and disrupt the exploitation of individuals as money mules.

To find out more visit: austrac.gov.au/smr.

FOR MORE INFORMATION

If you have questions about your AUSTRAC compliance obligations, please email contact@austrac.gov.au or phone 1300 021 037.

AFP News & Media -
Borders opening: Money mules beware [3]

WHEN TO SUBMIT AN SMR TO AUSTRAC

If you see something suspicious and report it to police, you must also report it to AUSTRAC.

You must submit an SMR to AUSTRAC if you suspect on reasonable grounds that a customer is not who they claim to be, or the designated service relates to terrorism financing, money laundering, an offence against a Commonwealth, State or Territory law, proceeds of crime or tax evasion.

3 afp.gov.au/news-centre/media-release/borders-opening-money-mules-beware

AUSTRAC.GOV.AU

1300 021 037

contact@austrac.gov.au