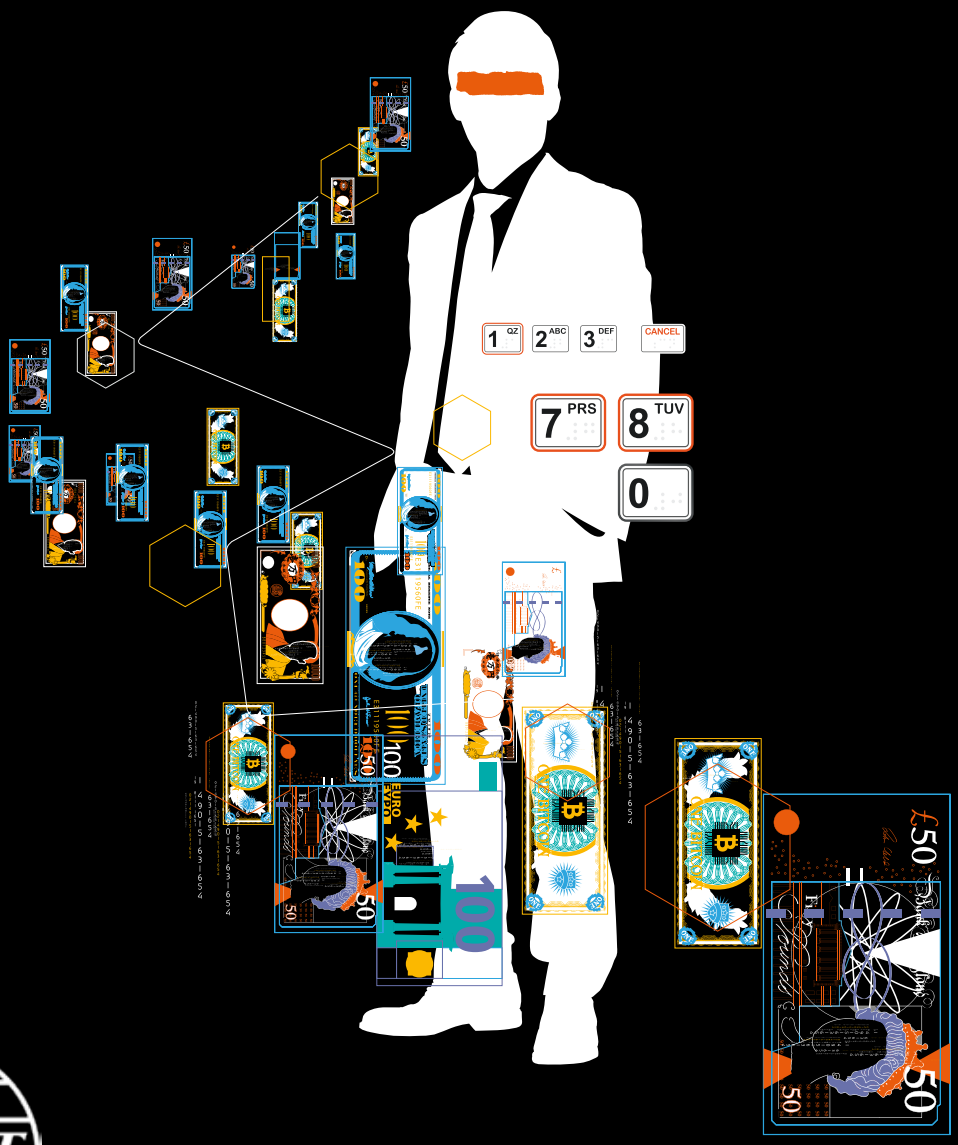
Understanding the money laundering techniques that support large-scale cyber-heists

Follow the Money

baesystems.com/SWIFT



SWIFT

BAE SYSTEMS

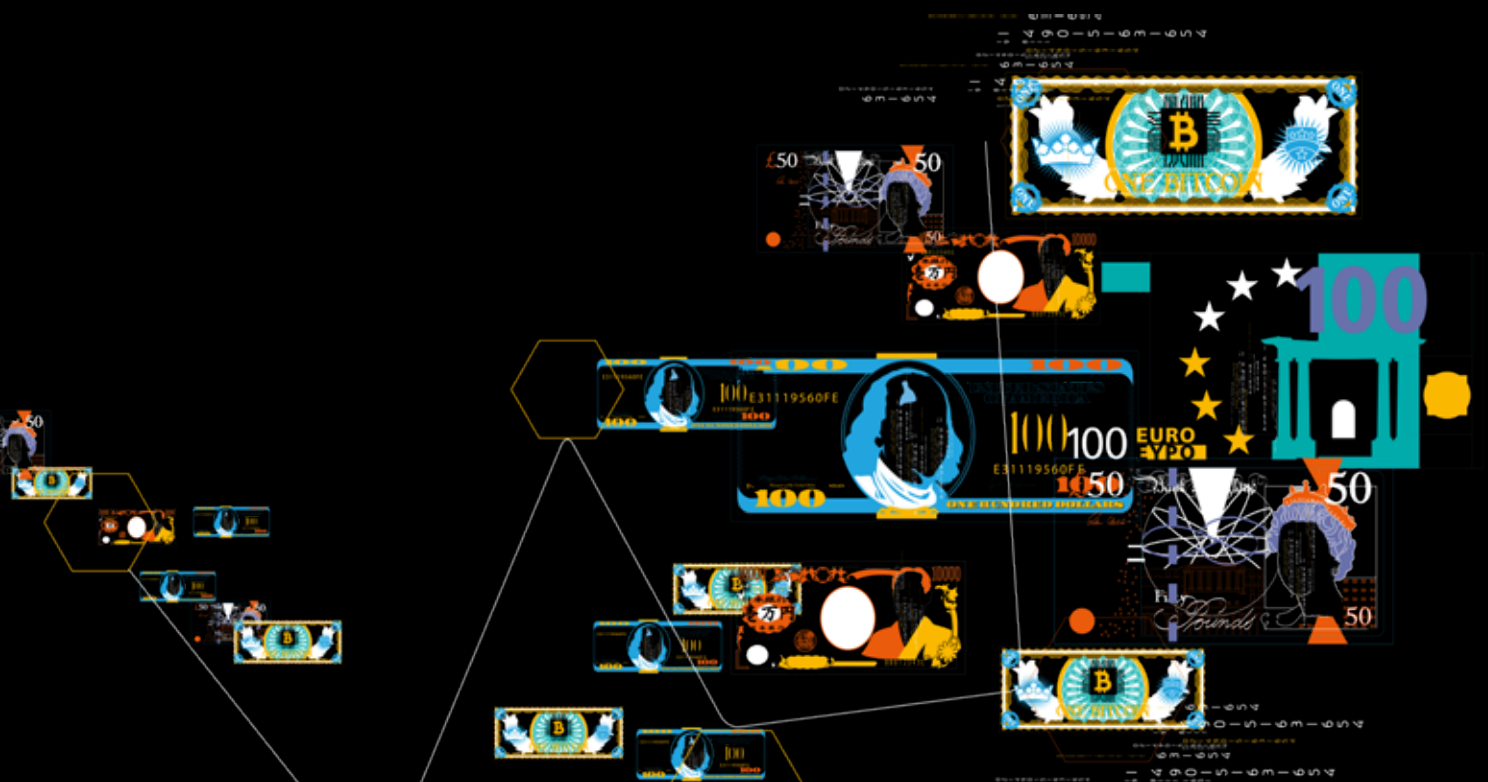
I. Summary

SWIFT plays a key role in helping its community to reinforce and safeguard the integrity of the global financial ecosystem, and maintains a relentless focus on security. As part of that focus, SWIFT has an ongoing commitment to intelligence sharing and thought leadership that contribute to the community's understanding of the cyber threat and tactics of cyber criminals. One area where the community has expressed interest in gaining more insight is around the approaches cyber criminals use to extract money once they have executed a successful attack. With this in mind, SWIFT commissioned BAE Systems to research and write this report. Its aim is to illuminate the tactics and techniques used by cyber criminals to cash out so that the SWIFT community can better protect itself, through both cybersecurity controls and financial crime compliance processes.

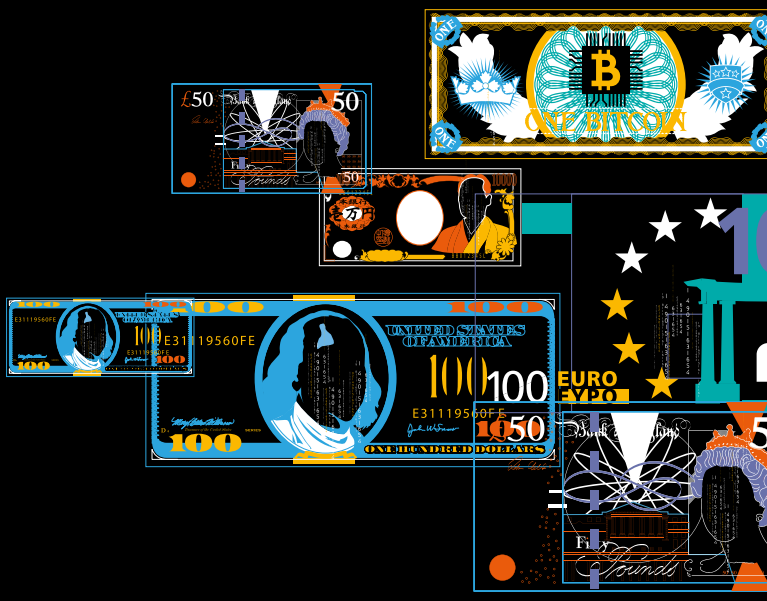
Large scale cyber heists, in which cyber-attackers manage to steal significant amounts of money from banks, continue to create news headlines. Various reports have been produced previously on how some of these attacks, such as those against banks' high-value payment systems, succeed and how organisations can mount better defences. BAE Systems and SWIFT have jointly published reports on cyber heist techniques used against financial institutions and the evolution of the cyber threat to the banking community in 2017[1] and 2019[2] respectively.

However, to date, there has not been significant material published on what happens to funds after they have been stolen. This report focuses on that area, specifically the money laundering related activities necessary for cyber-attackers to not only conduct and 'cash out' a successful attack but also avoid the money subsequently being traced.

This report describes how money laundering is typically performed in the context of large-scale cyber heists. It illustrates key parts of the typical processes used by cyber-criminals with examples to help better inform readers on areas they should focus on to better prevent, detect and respond to money laundering. In addition, the report offers perspectives on areas in which controls could be further improved and how money laundering techniques may evolve.



"...there has not been significant material published on what happens to funds after they have been stolen. This report focuses on that area..."



1 https://www.baesystems.com/en/cybersecurity/feature/the-evolving-cyber-threat-to-the-banking-community

2 https://www.baesystems.com/en/cybersecurity/feature/the-evolving-advanced-cyber-threat-to-financial-markets

2. Introduction

The activities of all cyber-criminals, whether working individually, as part of a small gang, as organised crime groups, or even for a nation state, have resulted in annual total cyber-crime revenue estimated at USDI.5 trillion[3]. Banks remain a prime target for cyber-criminals because they are critical infrastructure that can facilitate direct access to cash/funds.

The financial industry, however, is not an easy target. Banks, law enforcement and industry bodies continue to evolve cyber defences, improve information sharing, and regularly prevent money from ultimately being stolen even when the first stage of a cyber-attack may have seemed successful. Cross industry efforts such as SWIFT's Customer Security Programme (CSP), which provides tools, information and a framework to help the SWIFT community secure itself, and payments screening services continue to evolve to mitigate cyber-attacks. For example, 91% of SWIFT customers, representing 99% of SWIFT traffic, attested to their compliance with controls set out by the latest Customer Controls Security Framework, a set of security controls which serve as the cornerstone of CSP. In addition, banks have improved response security controls such as the ability to stop or recall fraudulent payment instructions where these are identified quickly enough.

However, the lure of targeting banks to get ready access to cash remains prevalent, and attackers continue to develop their techniques. In recent years, many attacks have moved from targeting high-value payment systems to targeting ATM networks and related systems. While these may, on the face of it, seem to have a lower inherent value as any ATM inherently holds a limited amount of cash, in terms of successfully obtaining multi-million dollar sums of money across a number of attacks, this has to date proved to be a successful alternate route for attackers.

But irrespective of the cyber-attack method, the challenge all criminals face after a successful cyber-attack is getting hold of cash or other liquid financial assets that are perceived as 'clean', i.e. where it is not possible to tell it is from the proceeds of crime. This is where the need for money laundering comes in.

The money laundering and associated techniques described in this report are those considered relevant to large-scale cyber heists against banks' high-value payment systems and ATM related systems, including back-office payment systems. Such cyber attacks involve being able to manipulate or subvert the correct operation of high-value payment systems or management systems controlling a number of ATMs. This paper has not specifically considered what happens to money stolen in other financial crime related attacks such as physical attacks against individual ATMs, card skimming and cloning, banking Trojans and malware, authorised push payment or business email compromise type attacks. However, the money laundering techniques and controls described are likely to also be relevant in many of these cases.

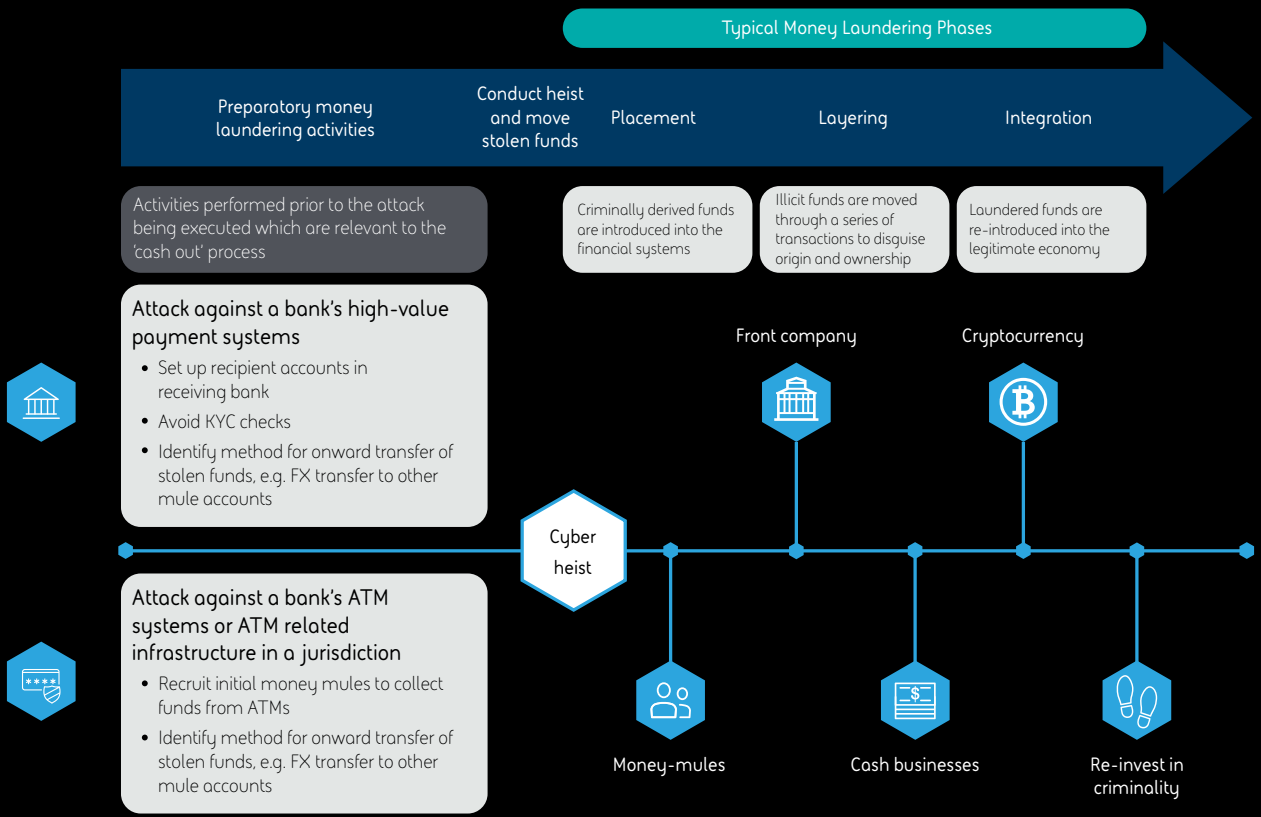
3 https://www.experian.com/blogs/ask-experian/cybercrime-the-I-5-trillion-problem/

3. Money Laundering Overview

In the strictest sense, money is laundered whenever a person or business deals in any way with another person or organisation's benefits from crime. Traditionally, money laundering has been described as a process which takes place in three stages: placement, layering and integration:

- Placement – Criminally derived funds are introduced into the financial system in the case of an ATM style attack, or, in the case of a cyber heist against a bank's high value payment systems; placement covers the initial fraudulent movement of funds
- Layering – Illicit funds are moved through the financial system in order to disguise their origin and ownership. This is the most substantive phase of the process
- Integration – Laundered funds are re-introduced into the legitimate economy, or reinvested into the criminal enterprise

Various methods underpin how funds are typically removed from a bank during a large-scale cyber-heist, as well as the money laundering techniques that aim to conceal their subsequent movement. There can also be significant overlap between the money laundering phases in reality.



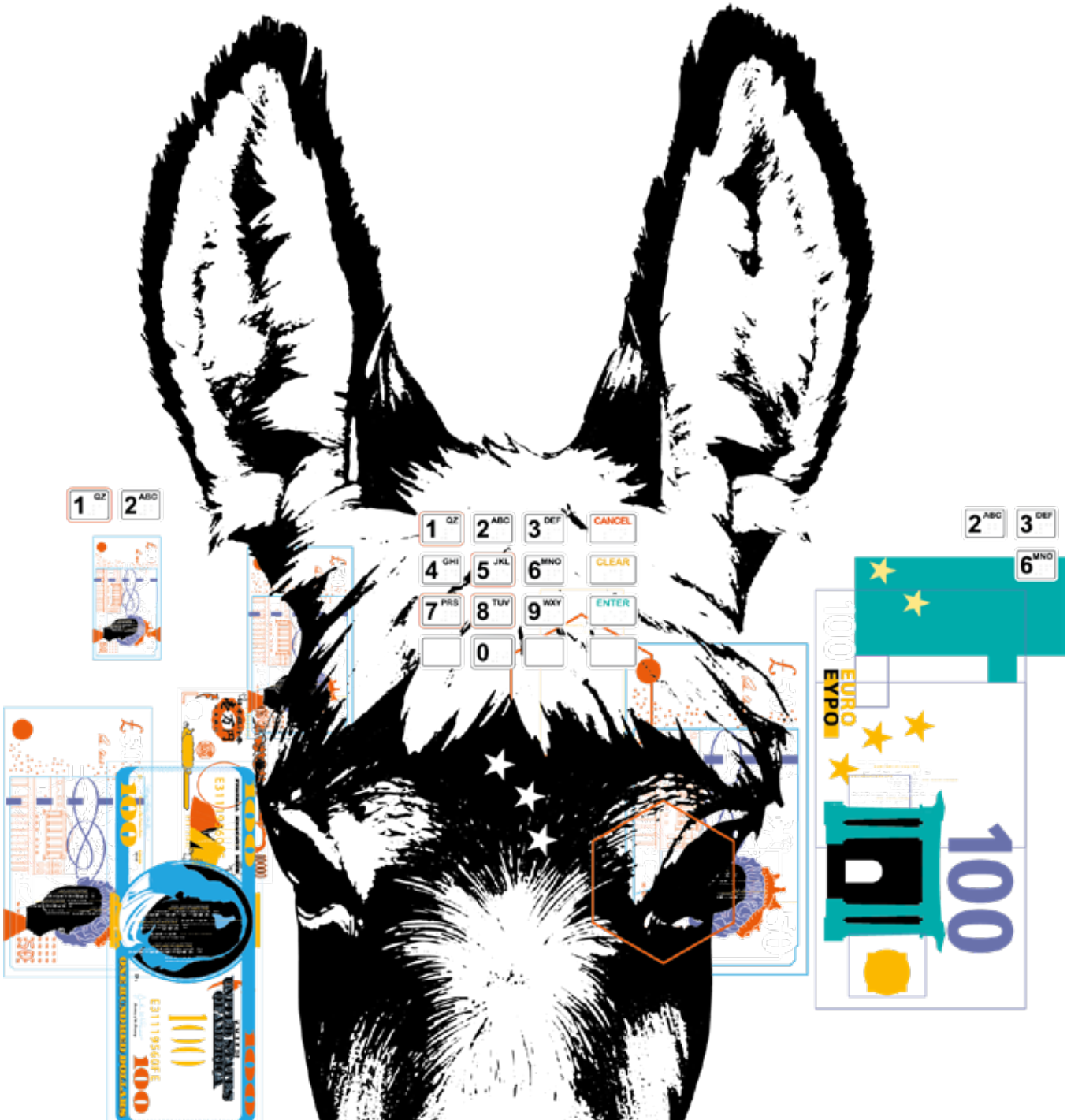
The following sections describe each of these four money laundering related phases in more detail, covering:

- Preparatory activities
- Placement
- Layering
- Integration

3.1 Preparatory Activities

For large-scale cyber heists to be successfully executed, attackers need to perform a number of steps in advance. Outside of those relevant to successfully conducting the cyber element of the heist, which are not the focus of this paper, money laundering steps the attackers need to complete include:

- Setting up or gaining access to bank accounts into which stolen funds can be initially received, or in the case of ATM-related heists, the attackers need to recruit and train money-mules to take the stolen cash out of the ATMs
- Recruiting money-mules to transfer the stolen funds out of those accounts



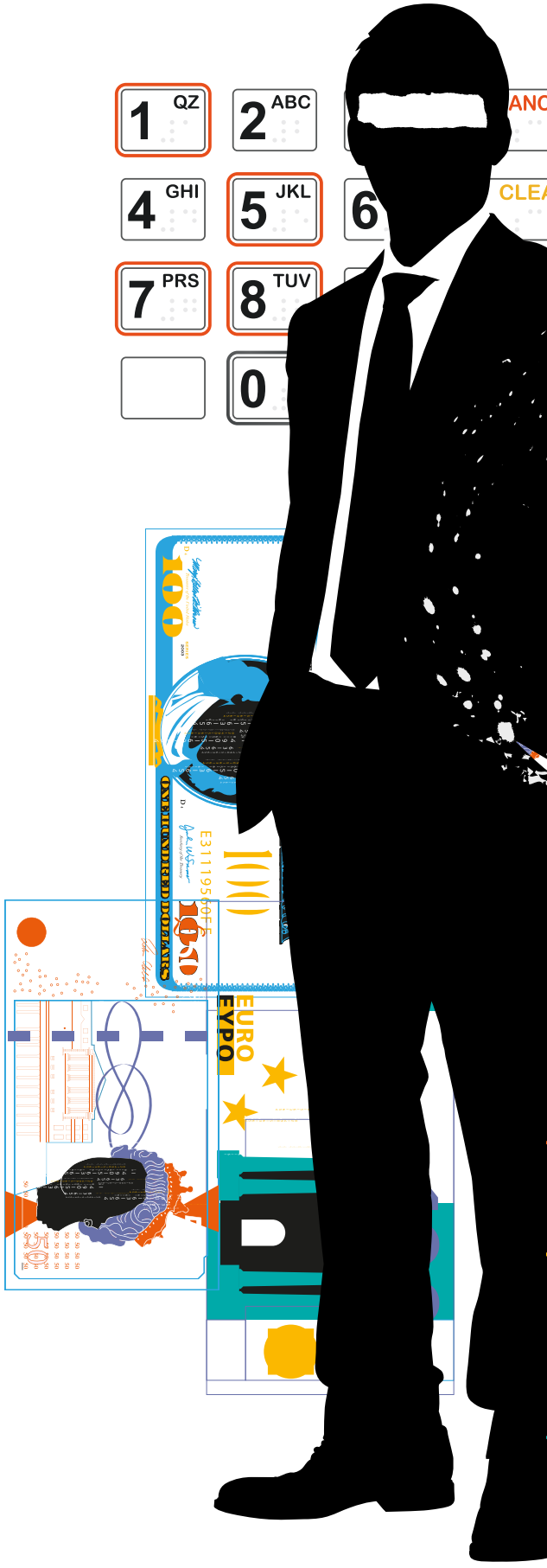
3.1.1 Account set up

- Setting up accounts to be used in a cyber-heist is a key step as these accounts will be the destination of the funds after they have been stolen, also known as the 'end-beneficiary'. There have been many instances where these accounts have been set up in good faith, believing that the account holders are genuine and of decent integrity, due to the use of false identification documents or by using legitimate identification documents from individuals who have been coerced by criminals to allow the account to be used. There have also been instances where existing accounts were used – for example where an individual who no-longer has a requirement for their valid account hands it over to someone else, rather than closing it. The establishment of these fraudulent accounts, by whichever method, might be facilitated by weak or ineffective policies and controls linked to the customer due diligence processes and also by lack of training of front-line staff.

- In order to avoid suspicion, fraudulent accounts might be set up several months before the heist, and so are empty and unused. Assigning fake projects and companies to these fraudulent accounts serves the purpose of giving credibility as well as explaining why, at some point, they will be in receipt of large money transfers. In line with this, as an additional obfuscation technique, accounts linked to fake organisations may be set up to be used as a hub and collation point for stolen funds after they have been transferred to the initial fraudulent accounts.

- The effectiveness of a financial institution's Know Your Customer (KYC) and screening processes are also important factors – and is likely why certain institutions in certain jurisdictions are targeted for illicit activity. The 'Know Your Customer' process is a vital part of validating users - from simple name screening and undertaking background checks through to enhanced due diligence (EDD) with independent assurance provided by two person validation to provide greater level of scrutiny. If these processes are weak or ineffective, or if the staff is poorly trained, then this allows these checks to be ineffective. Furthermore, there have been cases where a complicit or coerced insider has helped to evade or reduce the scrutiny of compliance teams carrying out KYC and due diligence checks of new account openings.

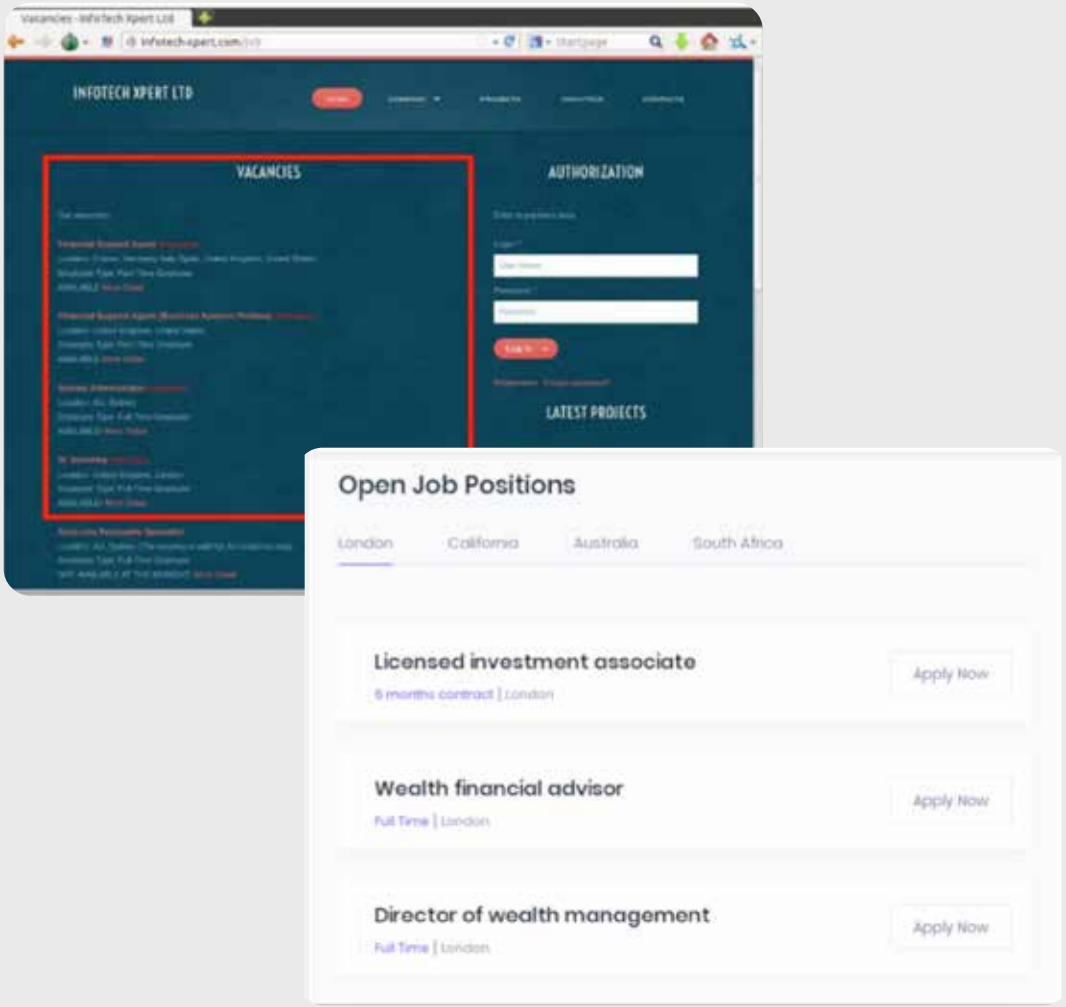
- For ATM cashouts, the nature of account set-up differs depending on the type of method used.
    - ATM FASTCash involves the fraudulent duplication of legitimate cards, which requires cyber-criminals to access customer records in order to create a duplicate card.
    - ATM cashouts involve an insider creating a phantom transfer of funds to accounts that are owned by recruited money-mules. In order to create a layer of obfuscation, fake identities are used for these accounts so that the mule's identity is concealed.
    - ATM management cashouts that involve a cyber-intrusion which remotely controls ATMs do not require accounts to be set up to carry-out the heist.



3.1.2 Recruit money-mules

- A common denominator that underpins cyber-heists is the essential function of the money-mule – irrespective of the diversity of the cyber-crime group, the execution of the heist, or the final destination of laundered funds. Their role seeks to provide the obfuscation in the chain between the initial fraud in the bank and the transfer of stolen funds to cyber-criminals. Accounts used for money-muling may be created by those complicit in the criminal activity or may belong to unsuspecting individuals tricked into allowing their account to be used for criminal purposes. These are the various actions that would qualify as a money-mule supporting cyber-heists:
    - Someone's bank account being controlled and taken over by a cyber-criminal / selling control to a cyber-criminal.
    - Receiving funds into a bank account before onward transfer to a cyber-criminal.
    - Using a fake identity to open an account for the sole purpose of benefiting a cyber-criminal.
    - Re-shipping items purchased by a cyber-criminal using stolen banking details.
    - Collecting stolen funds via ATM cash outs.

- Cyber-criminals have become more creative with their methodologies for recruiting money-mules. Some cyber-criminals often dupe innocent victims into laundering money on their behalf with the promise of easy money by using seemingly legitimate job adverts, online posts, social media and other methods. This includes incorporating aspects like diversity and inclusion (D&I) into job adverts to encourage a person to believe the company is real, as well as creating fake management teams. Some job adverts appear to be targeted towards people based in countries that are not typical financial targets, (e.g. UK, US, and Australia). For cyber-criminals in Eastern Europe this recruitment technique serves as further obfuscation, due to international transfers increasing the complexity.
- Many money-mule recruitment efforts focus on individuals, especially young adults including those seeking to fund higher education and adults recently out of work, who are likely to jump at the chance to apparently easily earn extra cash. Some examples of money-mule related job adverts are shown on the following page, indicating that in many cases, the money-mules are not strongly linked with the cyber-attackers.



Employment Type: Contract position
Salary: We are offering an 6 hour shift, 5 days per week with compensation $9,500.00 per month + commission.

The job advert contains the following description of responsibilities in the role:

Your work includes contacting potential investors on a particular projects via the communication means (e-mail, phone); discussion and explanation of all the details of the proposed projects; assistance in the choice of the right projects for the investment, ensuring of the convenient methods of the investment between the investor and the developer company. We will provide you the database of the investors and companies with whom you will work.

- Some cyber-criminals that are part of a large organised crime group are able to draw upon a cadre of associates for money-muling purposes. For nation-state cyber-groups which specialise in the ATM FASTCash technique, their links with various criminal groups in East Asia are utilised in order to recruit money-mules to travel to specific locations in order to withdraw cash from ATMs.

3.2 Placement

Placement involves the initial movement of stolen funds into the financial system. This can be the initial account into which stolen funds are transferred, or in the case of large-scale ATM based heists, the method of converting the cash obtained in a local currency into a more transferable currency, such as USD$.

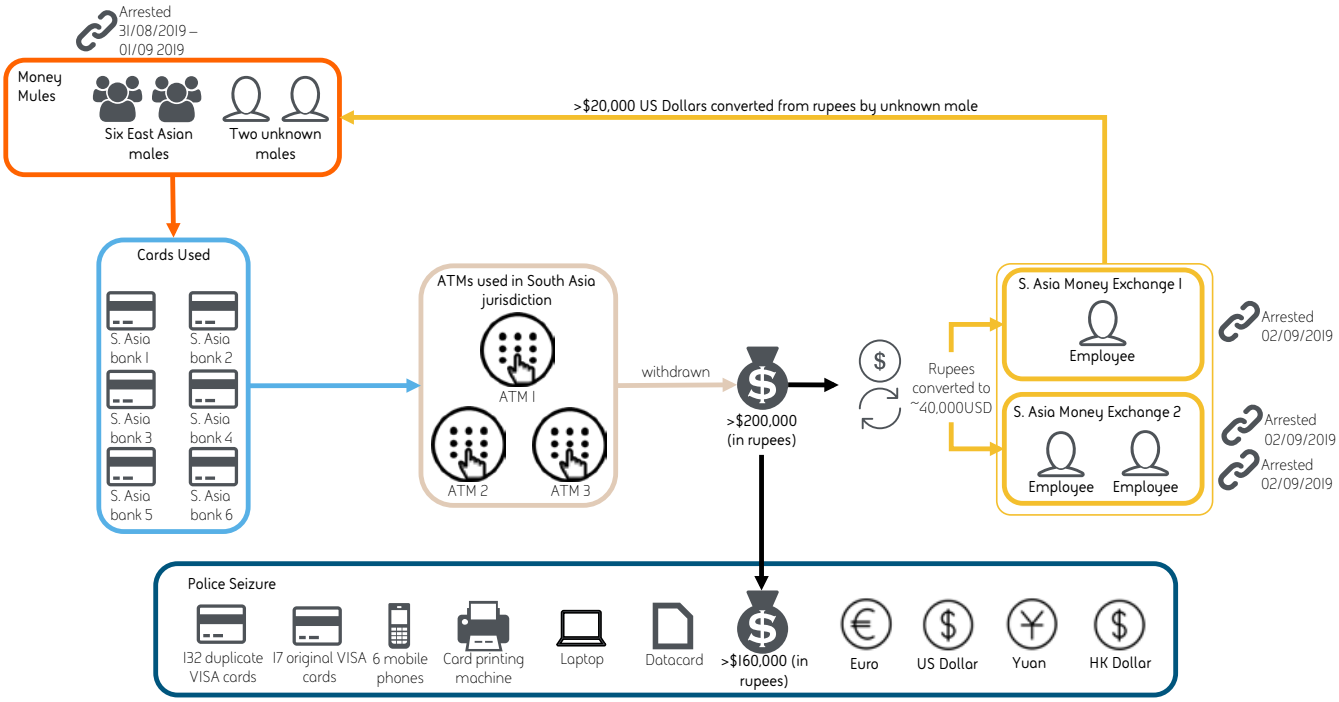
3.2.1 Use of Money-mules

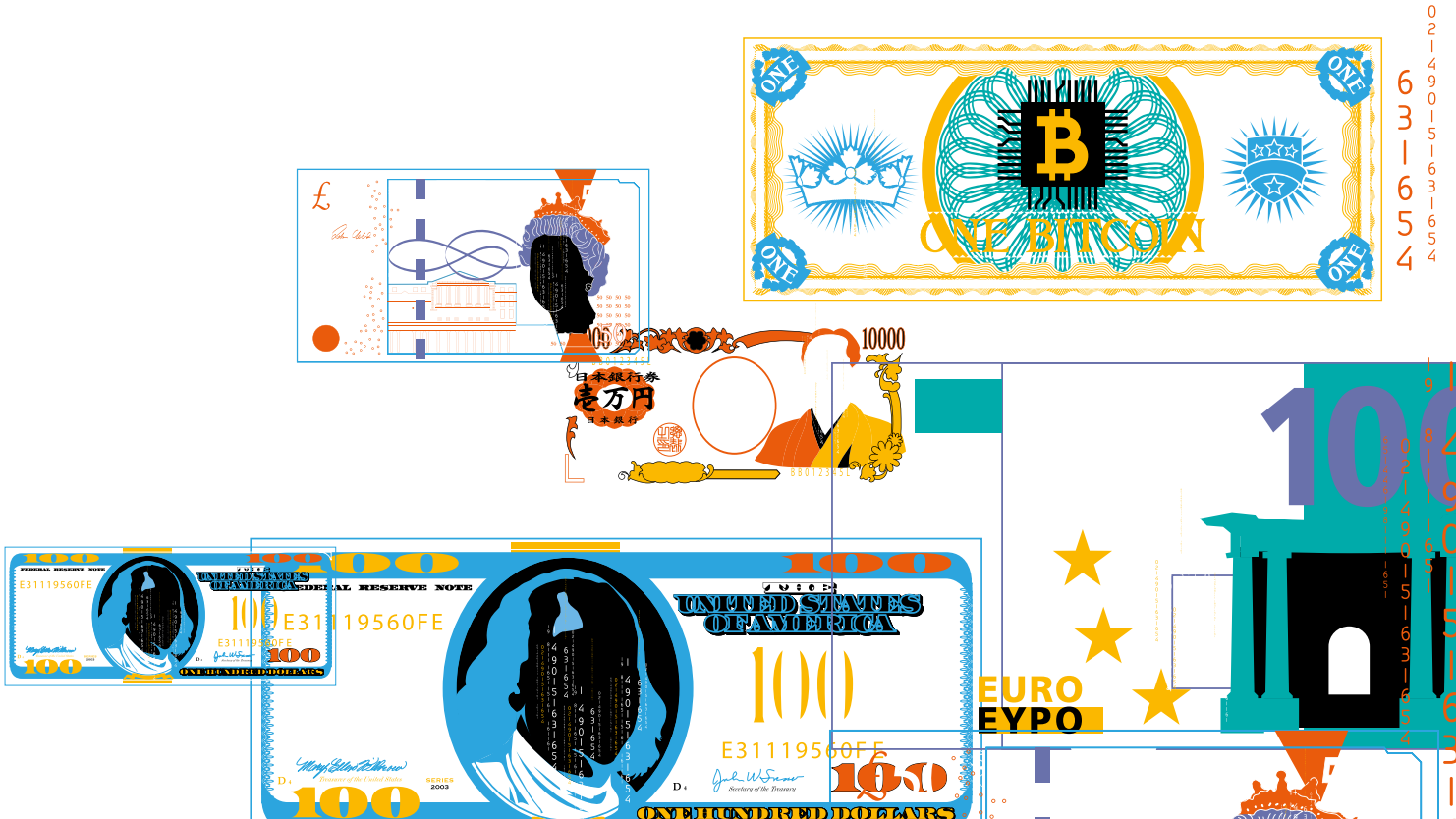
Money-mules serve as intermediaries for cyber-criminals and criminal organisations, where they act as a bridge between the exfiltration of stolen funds from a bank to transferring these funds to criminal benefactors. In this way, the money-mule is the essential first step in the placement of criminally derived funds into the financial system.

The number of money-mules involved in placement activities for a large-scale cyber-heist varies but has often been seen to involve around 10 individuals. However, there are of course exceptions to this. For example, an attack against one bank which is considered to be linked to the Lazarus Group involved 12,000 ATM withdrawals being performed in approximately a two-hour timeframe across 28 countries, pointing to a large and organised group of money-mules being involved.

It should also be noted that other money-mules will likely be used further along the money laundering chain, with multiple sets of mules being used to obfuscate the source of the stolen funds, and thus their total number may be much higher than those involved in the initial placement activity.

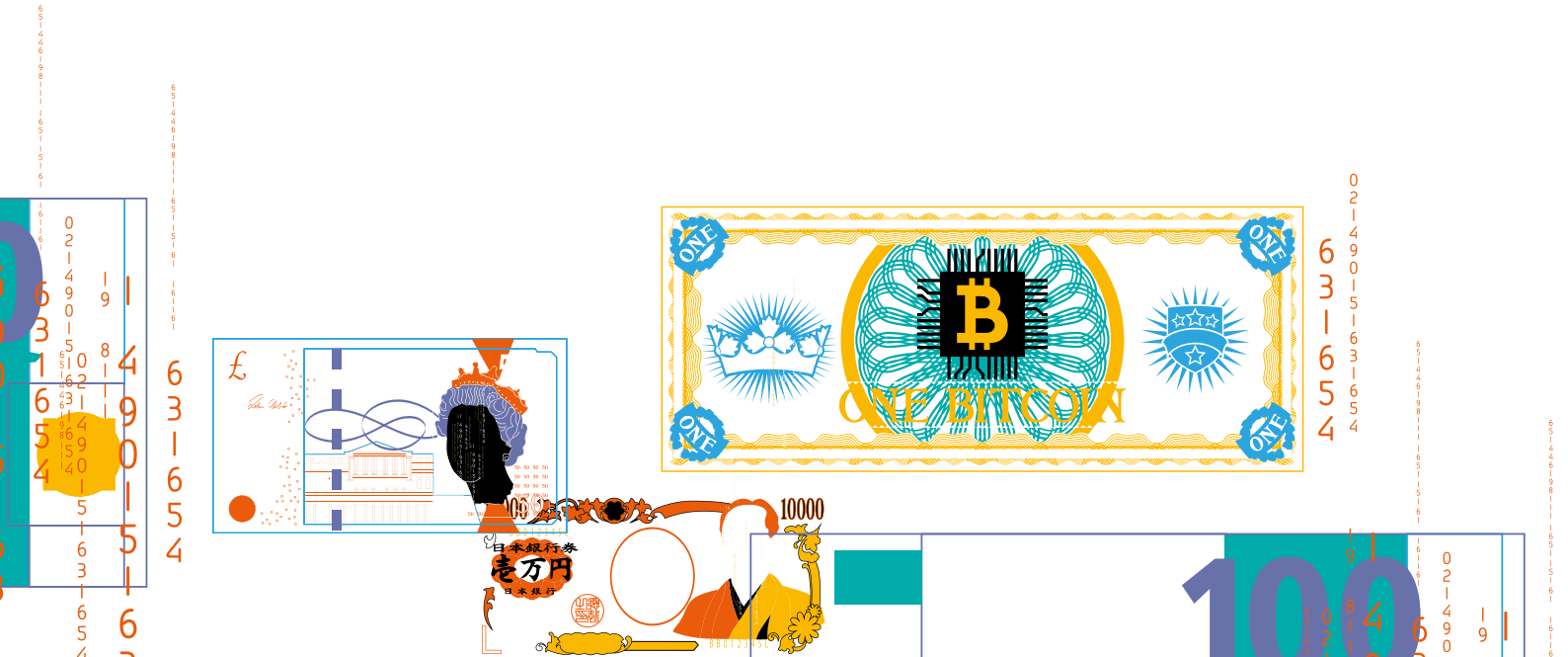
The following schematic provides an overview of a real-life ATM focused cyber-heist, outlining the number of money-mules involved and the initial mechanisms used to start the money laundering process.





The following schematic provides an overview of another real-life ATM focused cyber-heist, outlining the timeline of the attack and details on the money-mules involved in the initial placement.

Mid-September, 2019	Bank in the Balkans seen beaconing to Command and Control server of a cyber criminal group
Thu 3 October, 2019	Personal details of up to 60 million credit card holders leaked and sold on the black market
Fri 6 December, 2019	Two Eastern European males enter jurisdiction in the Balkans
Sat 10 December, 2019	Two Eastern European males leave jurisdiction in the Balkans
Fri 31 January, 2020	Same two Eastern European males enter jurisdiction in the Balkans with an accomplice
Fri 31 Jan – Sun 2 Feb, 2020	23 ATMs in the Balkan jurisdiction emptied over 53 hours. Quantity of Convertible Marka (KM) stolen.
Sun 2 February, 2020	Two original Eastern European males stopped and detained by local law enforcement, who inform the bank. The accomplice escapes.
Sun 2 February, 2020	A quantity of Convertible Marka (KM) is found on the two detained males. However, the majority of the amount stolen is unaccounted for.
Mon 3 February, 2020	The accomplice arrives at a Central European jurisdiction, and to date is still at large.
Mon 3 February, 2020	Law enforcement claim the group could be larger and that the total amount stolen in Convertible Marka (KM) is almost 3 times that declared during the heist of 31 Jan – 2 Feb 2020.



3.2.2 Risk of money muling

Despite being financially rewarded for their part in carrying-out a successful cyber-heist, the intrinsic risk associated with a money-mule is significant. In the event of an investigation by law enforcement and the authorities after a heist, the actions of the money mule are at the front line of the heist. Issues during the money-mule stage have led to the ultimate arrest of cyber-group leaders; however, it can often be the case that money-mules are the scapegoats, punished for their involvement, whereas the rest of the cyber group remain at large[4].

The process of money-muling marks the most physical aspect of an ATM related cyber heist, which is why it might be considered to be the weakest link in a cyber-heist, as well as underlining the risk associated with money-muling at an ATM. CCTV cameras that are often present at ATM locations offer the chance to identify and record suspicious behaviour and capture facial features that could in some circumstances be cross referenced with law enforcement or border control data. The methodologies that underpin the various ATM cashout techniques carry certain risks. The lack of a card and pin entry associated with the ATM management technique has been noticed as suspicious by law enforcement, and has led to the arrest of money-mules. Similarly, the speedy draining of cash from ATMs, which were targeted by a FASTCash theft was identified as unusual by banking staff and led to the subsequent arrest of money-mules.

3.2.3 Money-muling interventions

Many initiatives that look to mitigate the risk of successful cyber-heists focus on money-mules. At the end of 2019, law enforcement authorities from 31 countries, supported by Europol, Eurojust and the European Banking Federation (EBF), came together to support the fifth coordinated global action against money muling, with the European Money Mule Action[5]. In the period between September and November 2019, this resulted in the identification of 3833 money-mules alongside 386 money-mule recruiters, of which 228 were arrested. More than 650 banks, 17 bank associations and other financial institutions helped to report 7520 fraudulent money-mule transactions, preventing a total loss of €12.9 million.

4 https://www.nationalcrimeagency.gov.uk/news/arrests-in-belfast-and-london-in-cyber-heist-money-laundering-investigation

5 https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering

"The European Money Mule Action (EMMA) shows how a close public-private partnership between law enforcement, judicial authorities and the banking sector is essential to effectively tackle the illegal activity of money muling."

Europol-Eurojust-European Banking Federation (EBF)

3.3 Layering

Layering is the most substantive phase of the money laundering process, involving multiple steps to conceal the origin and ownership of the stolen funds.

3.3.1 What happens after the funds are with the initial money-mule?

Monies withdrawn from ATMs in cyber-heists tend to be immediately exchanged into US Dollars at money exchanges. This step in the process could suggest complicity by employees at money exchanges to support a money laundering process, albeit via a bribe, or it could indicate negligence. Although in some cases the initial money-mules have been caught, in others where the heist has been successful, e.g. after the money-mule has withdrawn funds from an ATM, they might be passed onto an intermediary who, in turn, passes the stolen funds to the cyber-criminal. However, in some instances, especially after cyber-heists relating to nation state actors like the Lazarus Group, it might be the case that the fate of these stolen funds is to be channelled via other layering techniques in order to further obfuscate the path of the stolen funds.

Out of all attempted Lazarus heists, a subset showed successful fraudulent transactions with a majority of transfers being sent to East Asia, where there are numerous linked front companies.

3.3.2 Obfuscation of funds via front companies

The setting up of front companies can be used by some jurisdictions as a method to circumvent the adverse impact of imposed sanctions and to enable covert access to the global financial system. It also facilitates the potential for obfuscating the flow of money and concealing various techniques for money laundering. Front companies are corporations that act as a 'cover' for the laundering of illicit funds and typically lack significant legitimate assets. They either do not maintain active business operations, or, in some instances, the front company can have a legitimate purpose, which is used as an effective way of concealing the true ownership of businesses and accounts, as well as associated assets and parties. In this way, front companies can be an effective entity through which illicit transactions can be circulated and consequently obfuscated. Front companies are often set up in jurisdictions that are known for strong banking secrecy laws or for poor enforcement of money laundering regulations, as these are preferable for individuals with illicit intentions.

3.3.3 Cash businesses

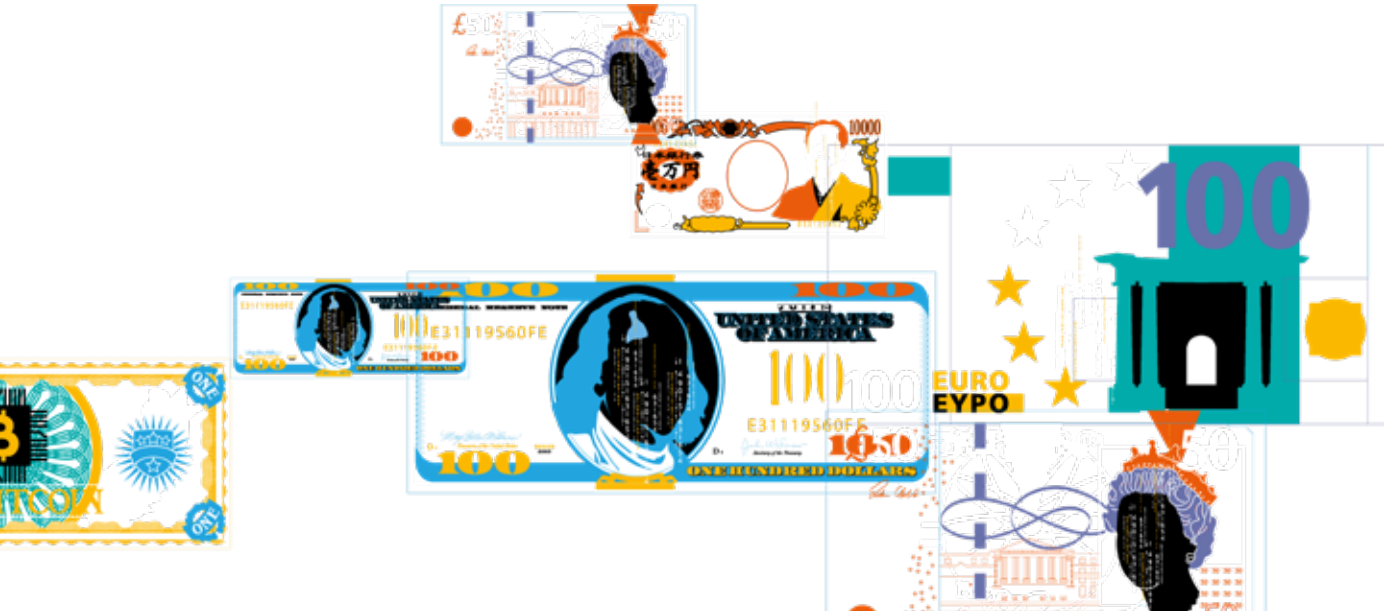
Cash intense businesses can refer to high end luxury goods markets, such as the gold market, and the diamond and jewels industries as well as more generic businesses like betting shops, casinos, or other services. As these industries transact mainly in cash, they can offer a mechanism for laundering the proceeds of a crime. Casinos are significant cash businesses and can be used by a launderer to clean cash by converting it into chips at a casino, and then exchange it back into cash to deposit at a bank, and have a cheque from the casino showing a legitimate transaction. The fact that in some jurisdictions names are unregistered and winnings unreported have made casinos an attractive method for laundering stolen funds.

3.3.4 Use of financial representatives

Front companies registered in East Asia are considered to operate on behalf of the government of a FATF high risk jurisdiction. In one instance, a front company was accused of laundering more than USD$100 million for the sanctioned state-run bank of a FATF high risk jurisdiction. Financial representatives using East Asian aliases, or in close liaison with facilitators in East Asia, are responsible for setting up and operating front companies and bank accounts across the East Asia region. These front companies and relationships offer a method of laundering the proceeds from a cyber-heist in order to expedite and obfuscate the process of stolen funds being used for nefarious purposes, such as purchasing equipment to bypass sanctions. In one example front companies import natural resources without making any prepayment. These organisations resell the natural resource to customers across Asia, retaining the US Dollar proceeds. Rather than sending funds to the FATF high risk jurisdiction, the following obfuscation stages occur:

- The payments received by this organisation from customers are processed via banks in East Asia and diced up into smaller outflows (minus a fee for facilitating the sale). This forms part of an intricate layering scheme directed to front companies and shipping or trade businesses typically registered in jurisdictions in East Asia. Financial representatives are key to establishing the front companies and making the transactions appear legitimate.

- The FATF high risk jurisdiction sends instructions to the front company of items it would like to purchase. The front companies then use the received payments to purchase and ship commodities. Items purchased can range from bulk commodities, luxury items, electronic items as well as equipment. It is assessed that items used could be smuggled with other non-suspicious shipments.



3.3.5 Red flags

Red flags relating to front companies that are involved in illicit financial activity are:

- Financial activity by a front company that has no relevance to its stated area of business
- Evidence of shared entities between front companies, including addresses, phones numbers, managers and owners
- Front companies that lack obvious public activity or presence
- Business types cited for front companies involved in illicit activity are often textile, garment, fishery, and seafood businesses.

These red flags could assist individuals in financial institutions working on areas of compliance like due diligence and KYC screening to better detect front companies used for illicit purposes.

3.3.6 Facilitating jurisdictions

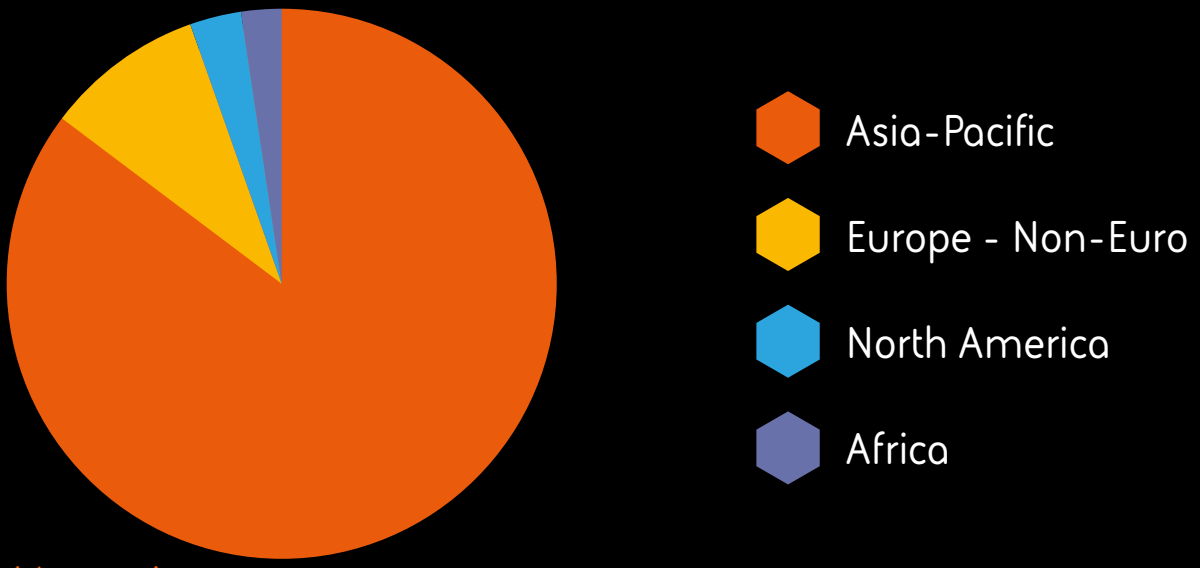
Regulations and conditions that govern company registration and reporting requirements in East Asia make the region an attractive place to do business, as well as vulnerable to being abused. In some of the region's jurisdictions, a company's registered office must be there and it is permitted to share an office with their company secretary, but neither technically has to operate out of that address. This loophole, which would typically be considered as a red flag for money laundering investigators, underpins how nefarious activity is facilitated, since it has enabled the creation of vast numbers of front companies. This explains why this hub has been attractive for heavily sanctioned jurisdictions seeking to access international trading markets and to facilitate money laundering.

East Asia can also serve as an effective gateway that offers sanctioned jurisdictions access to US Dollars, via clearing services offered from some jurisdictions, potentially providing a route that might enable oversight for payments between banks using US Dollars to be circumvented.

"The East Asian international financial hub has company formation and registration rules that we think need to be stronger...It is important it has mechanisms and regulations prohibiting activities that facilitate financial transactions with a FATF high risk jurisdiction."

U.S. Treasury's Under Secretary for Terrorism and Financial Intelligence

Out of all attempted heists attributed to the Lazarus Group, a subset of cases showed successful fraudulent transactions. The graph below shows the locations of the beneficiary banks in successful cases in 2018. The majority of transfers are sent to East Asia, where mule accounts are accessed. The following details regions of recipient institutions in 2018, based on SWIFT data[6].



3.4 Integration

The means and methods by which cyber-criminals choose to convert stolen funds into an usable end product or asset can be a useful barometer of the strategic professionalism and experience of the cyber-attack group. It can also help the process through which law enforcement agencies might close in on the group.

3.4.1 Cash-out conundrum

The cash out process opted for by cyber-criminals (including those involved in precursor steps, money-mules, operating front companies, etc.) can reveal a strong correlation between the extravagant ways stolen funds are spent, and the professionalism of the criminal. Operations that were early in a cyber-criminal's history or were a one-off occurrence reveal an immediacy in how stolen funds are used – be it to clear a pressing debt or for materialistic acquisition. Such suspicious behaviour could be the first clue in linking them to the heist, which could ultimately start a trail that leads to members of the cyber-group being identified.

6 https://www.virusbulletin.com/conference/vb2019/abstracts/art-cashout-evolution-attacks-payment-systems

3.4.2 Integration of funds: cyber-criminals

Some cyber-attack groups have been seen to make many extravagant purchases, possibly borne out of inexperience, as it draws the attention of law enforcement agencies and often leads to the arrest of the cyber-criminals. An inability to use the funds more strategically with less ostentatious purchases is often their undoing. In other cases, the methods chosen to cash-out the proceeds of a cyber-heist illustrate greater experience and a strategic approach driven by wanting to maintain a low profile. Property and jewellery are investments that are likely to hold their value and potentially less likely to attract the attention of law enforcement.

3.4.3 Integration of funds: nation state actors

The independence and freedoms enjoyed by criminal cyber-groups are not shared by nation state cyber-groups. Far from their actions leading to materialistic acquisition and personal possessions, the purpose of these cyber actors is to fulfil the demands and wishes of the regime.

3.4.4 Reinvesting in criminality

As a final stage of money laundering, cyber-criminals might seek to integrate the proceeds of a cyber-heist by reinvesting in crime, especially in the illegal drugs market. Over a third of organised crime groups in Europe, including cyber-criminals, are directly involved in the production or trafficking of illegal drugs. Cyber-criminals have been known to operate websites, which facilitate the sale of illegal drugs, firearms, malicious software, hacking tools, stolen financial information, payment cards and other illegal counterfeit goods on a number of dark web marketplaces. In some instances, this activity can lead to kickback payments in bitcoin that is equivalent to several million USD$.

3.4.5 Cryptocurrency and its growing appeal

Identified cases of laundering through cryptocurrencies remain relatively small compared to the volumes of cash laundered through traditional methods. However, in one major case, a significant cyber-crime group is estimated to have converted stolen funds obtained from ATM cashouts into cryptocurrency. The raft of alternative cryptocurrencies that offer greater anonymity, as well as services like mixers and tumblers that help obscure the source of funds by blending potentially identifiable cryptocurrency funds with large amounts of other funds, could boost the appeal of cryptocurrency for nefarious purposes.

In one case that resulted in arrest and prosecution, authorities found 15,000 bitcoins valued at USD$109 million, two sports cars and jewellery worth USD$557,000 at the house of the group leader. The group was found to operate in a truly international manner: the bitcoin farm where the group mined bitcoin in order to launder the stolen funds from the heists was located in an industrial building in East Asia, while many of the group arrested originated from Eastern Europe and the leader enjoyed the benefits of the stolen funds in Western Europe.

For heavily sanctioned territories, like a FATF high risk jurisdiction whose modus operandi focusses on raising funds with minimal associated risk, cryptocurrency offers a different income stream to targeting banks and financial institutions. It has been shown how the Lazarus Group have harnessed East Asian facilitators[7] in order to launder funds after a heist at a cryptocurrency exchange, using techniques that are similar to that described for heists from banks. The following summarises the process from the point of execution of the cyber heist:

- Lazarus Group steal funds in cryptocurrency from an exchange and stolen cryptocurrency is sent to multiple exchanges as a layering technique.
- East Asian facilitators, working on behalf of the Lazarus Group and the regime, receive a portion of the stolen funds.
- The East Asian facilitators transfer the cryptocurrency across addresses they hold, in order to further obfuscate the origin of the funds.
- East Asian facilitators move a portion of the received funds through newly added bank accounts that are linked to their exchange account – this enables the conversion from cryptocurrency into fiat currency. Other stolen funds might be transferred in Bitcoin into prepaid gift cards, which can be used at other exchanges to purchase additional Bitcoin.

Further insight into the money laundering methods used by the Lazarus Group is offered by activity after a cyber-theft at a cryptocurrency exchange in June 2018[8]. This resulted in the theft of USD$30 million in various crypto-assets. Subsequently, almost 2,000 Bitcoin was moved into a cryptocurrency exchange in Eastern Europe, over a 4 day period, involving 68 transactions. It is assessed that such a painstaking, strategic pattern of transactions is consistent with a desire to circumvent an exchange's anti money-laundering (AML) controls, including red flags associated with transaction limits.

7 https://home.treasury.gov/news/press-releases/sm924

8 https://rusi.org/publication/occasional-papers/closing-crypto-gap-guidance-countering-north-korean-cryptocurrency

3.4.6 Prepaid cryptocurrency cards

Cyber-criminals might seek to use cryptocurrency as a method for obfuscating and laundering the funds stolen during a cyber-heist, before making various purchases in order to integrate the funds. In this instance, cyber-criminals might launder the stolen funds at a bitcoin farm, before using financial platforms to load prepaid cards with bitcoin. Prepaid cryptocurrency cards can facilitate the reversion of cryptocurrency back into fiat currency in small amounts. This technique is enabled by a loophole so when the original financial institution issues the card, it does so in conjunction with the card issuer's partner – this partner company receive and convert the funds from cryptocurrency into fiat currency. The stolen money from several cyber-heists has in some cases been seen to be laundered via cryptocurrencies, using prepaid cards that are linked to cryptocurrency wallets. Financial platforms in Europe and the UK have been used to load prepaid cards with bitcoin, which were subsequently used to purchase jewellery, cars and property with stolen funds – those assets may sometimes then be subsequently sold, as a further money laundering step.

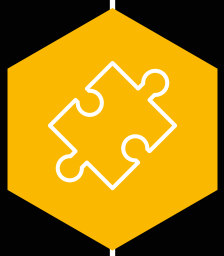
3.4.7 Converting cryptocurrency into tangible assets

An emergence of online marketplaces could offer effective methods for converting cryptocurrencies into tangible assets that can be held anonymously, or be sold as an extra step of laundering the proceeds of a cyber-heist. There are dedicated sites that facilitate the purchase of high-end land and property assets across the world, including luxury penthouses and tropical islands, as well as watches, jewellery, gold bars, and fine art. The concern for the financial system is that these digital transactions are conducted in a peer-to-peer manner that circumvents the checks and processes by banks, and often require only an e-mail address to make the purchase. This means that funds used to make a purchase that have been acquired by criminal means can be kept concealed.

4. Mitigation of money laundering risks

4.1 Information sharing technologies

A central initiative in empowering banks to be better able to detect illicit activity refers to them having more visibility of a greater pool of data. This is not only with regards to enhancing public-private sharing initiatives that foster better timely exchanges between financial institutions and law enforcement agencies, but also between financial institutions. In 2017, SWIFT created a global information sharing initiative, establishing a dedicated Customer Security Intelligence (CSI) team to investigate cyber incidents experienced by its customers and introduced a 'SWIFT ISAC' information sharing portal to share threat intelligence across the SWIFT member community.



Without amendments to legal and regulatory frameworks to enable banks to embrace advances in technology and data science to facilitate the safe sharing of AML information, identifying illicit behaviour will remain in their blind-spot until it's too late. The development of public-private partnerships to aid in the sharing of information between financial institutions and law enforcement has been mainly successful. There are also many technologies for enhancing information sharing between banks, including harnessing machine learning to enrich and make transaction and account monitoring programs more powerful and efficient. One approach that has been investigated by several banks is the use of Privacy Enhancing Technology, including homomorphic encryption, as a method of allowing queries to be run by one organisation on encrypted or open data sets held by other organisations in a privacy-enhancing manner to protect the nature of the queries being made.

4.2 Augmented sharing of risk factors pertaining to FATF high risk jurisdiction

A FATF high risk jurisdiction which conducts illicit practises via front companies in East Asia, in order to evade sanctions and launder monies, has been the subject of thorough investigations. However, there is a need to distil and cascade the key findings from such investigations across the international financial system. This will enable institutions to be more agile in identifying transactions that might relate to nefarious activity linked to a FATF high risk jurisdiction and trigger the need for enhanced due diligence. These refer to the presence of front companies in East Asia and the associated red flags that should alert suspicion. And given the activity of some diplomats from a FATF high risk jurisdiction to use accounts in the names of family members to evade sanctions and assist money laundering practises, these names could be shared with financial institutions to screen against as part of KYC and enhanced due diligence processes, as long as it is permitted by data protection and legal frameworks in various jurisdictions.

Similarly, augmented sharing of the red flags / situational circumstances that led to the successful arrest of individuals involved in the laundering stages of a cyber-heist could greatly increase awareness and agility in financial institutions and law enforcement agencies across various jurisdictions, which could ultimately lead to a reduction in vulnerabilities. Standard setting organisations, as well as regional Fraud Intelligence Units, could be effective conduits for such risk mitigating information sharing.

4.3 Money-Mule initiatives

The essential role of the money-mule in facilitating successful cyber-heists and enabling criminals to separate themselves from the fraud and the money laundering stages makes it an obvious focus area for risk mitigating initiatives. Numerous government, policing and industry initiatives have been launched, including:

- A series of coordinated actions by Europol's Cybercrime Centre (EC3), the Joint Cybercrime Action Taskforce (J-CAT), Eurojust, and the European Banking Federation have supported the European Money-mule Action initiative.

- Cifas, the UK's fraud prevention service have launched a joint campaign with Financial Fraud Action UK (FFA UK), which fights financial fraud for the UK payments industry, called the Don't Be Fooled campaign. This aims to deter young people – in particular students – from becoming money-mules.

- In December 2019, the U.S. DOJ and federal, state and international law enforcement partners announced a concentrated effort across the country and around the world to halt money-mule activity and shut down the enterprises that exploit the most vulnerable in society. The initiative aims to end the conduct of money-mules, as well as execute search warrants to secure evidence from money-mules who knowingly aided and abetted fraud schemes.

The success of funds-in-flight monitoring systems such as the Mule Insights Tactical Solution[9], that looks to augment the tracing of funds that are moved through the financial system, as well as initiatives like the European Money Mule Action that aims to identify and arrest mules, as well as engage with those most vulnerable to becoming a mule will be vital in preventing and deterring their viability. However, these initiatives will not address the risk posed by the rogue insider, who opens a bank account for the benefit of a cyber-criminal using a fake identity. This risk remains and is dependent on local regulators ensuring standards are maintained across financial institutions, as well as individual financial institutions regularly checking the integrity of employees' work and preventing accounts being set-up that are able to evade proper KYC processes and due-diligence screening.

9 http://www.fasterpayments.org.uk/press-release/new-anti-money-laundering-technology-sees-uk-fraud-rings-frozen

4.4 Compliance and reporting enhancements

There has been a tendency for cyber-heists to occur in jurisdictions where regulations are weaker, and there is a requirement for global standard setting bodies to do more in removing the platform for potential corruption. It is encouraging that some regulators in East Asia have set up a Fraud and Money Laundering Intelligence Taskforce in order to enhance the detection, prevention and disruption of money laundering. Other necessary requirements include tightening customer due diligence measures across financial institutions, to include the identification and verification of customers and the beneficial owner, as well as clarifying the purpose and intended nature of the business relationship. Enhancing reporting channels so that institutions can register their suspicions of illicit activity to a trusted and competent authority might also help to visualise networks of obfuscation and money laundering and identify criminal activity.

4.5 Insufficient cyber security

A pervasive issue across financial institutions is a reliance on legacy systems and processes. Often they have been spliced together through mergers, leaving them vulnerable to cyber-threat actors. Some cyber-security experts believe some banks are not investing smartly in maintaining systems and processes. Instead, they tend to focus on costly, complex, perimeter and device endpoint solutions, rather than focusing on investing in data centric security around main business assets and detecting abuse and intrusion by looking at the data and application layer. Financial institutions will continue to be vulnerable if they fail to identify and remediate network and application vulnerabilities before criminals have a chance to exploit them. Similarly, regular and updated staff awareness courses that help employees understand and spot risks relating to spear-phishing are simple initiatives that could pay dividends. For their part, augmented communication by regulators of usable cyber threat information that addresses security incident reports and systemic deficiencies could bolster cyber-security awareness across the financial sector.

"For too long, cybercriminals have exploited an international divergence in policy and legislation. I think we're now starting to see people coming together and understanding how to pool investigations together."

Head of Europol's European Cybercrime Centre

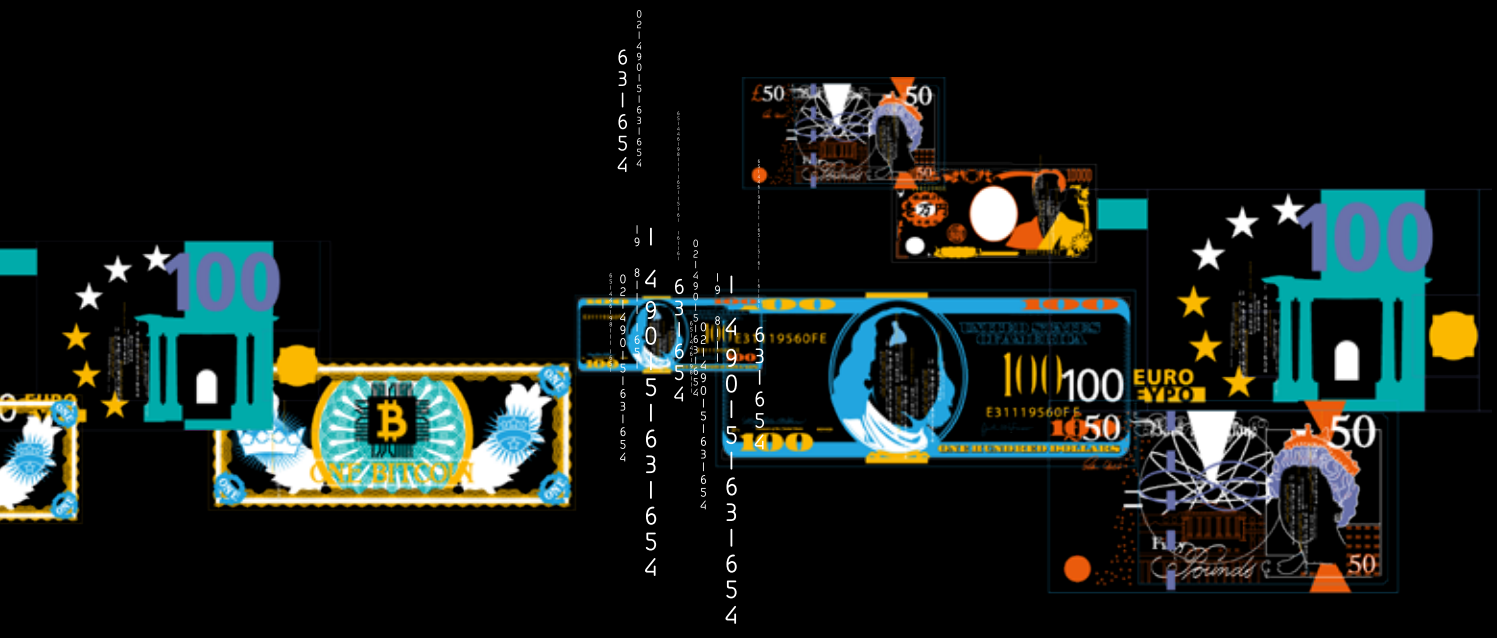
5. Conclusion

Large-scale cyber heist attempts are expected to continue and to evolve – the attackers are focused on going after large-scale payouts and will continue to mount attacks to achieve their aims. In addition, the desire to disrupt and destabilise the financial system, as opposed to just stealing funds should not be overlooked as an ongoing risk. Whereas many financial institutions are likely to be able to recover from just a financial theft, the distraction and destructive components of some techniques deployed by cyber-actors during a cyber heist are likely to have far greater operational impact. This can cost more to correct, as well as lead to a prolonged period of downtime for the financial institution, significantly impacting their customers and the institution's reputation.

Many cyber heists will continue to be detected and stopped, especially as financial institutions continue to improve their controls. However, financial institutions also need to ensure they don't become complacent. Threat actors have shown they will persist to seek to find ways around controls, including collaborating between groups where combining their skills will provide the desired reward for each threat actor.

Ultimately, some large-scale cyber heist attacks will unfortunately continue to be successful. Therefore, as money laundering is essential to a threat group realising the benefits of a successful large-scale cyber heist, a focus on seeking to disrupt criminal activity throughout the money laundering process should continue.

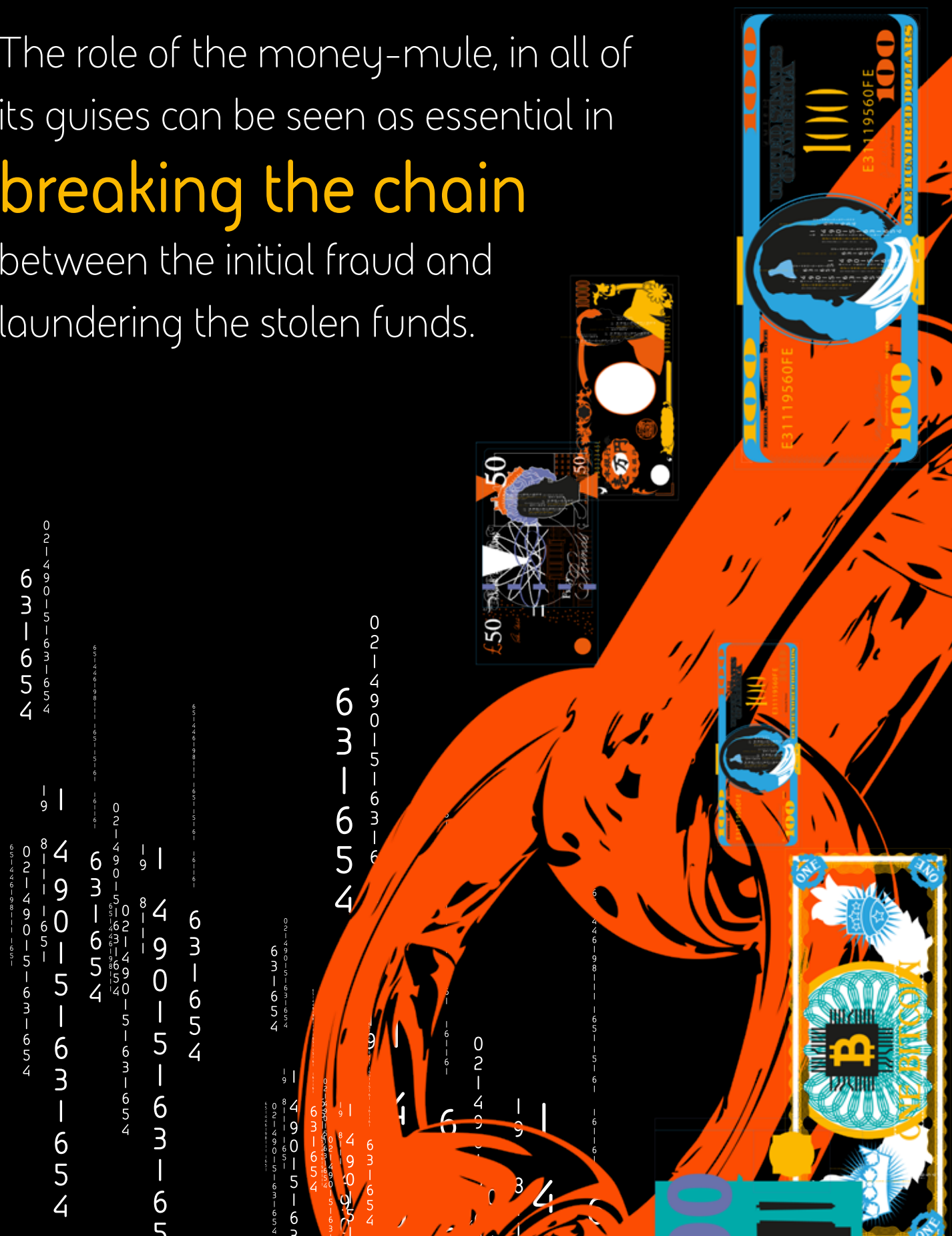
Threat groups will continue to collaborate throughout the money laundering lifecycle, leveraging the global criminal skillsets available and the willingness of many people to be tempted by the lure of an apparent quick and easy payday. Particular focus therefore should apply to the money-muling activities and also to the use of front companies. Collaboration will be key in these areas, both inter-organisational, within jurisdictions and internationally. In addition, awareness of new money laundering techniques, such as those involving cryptocurrency, will be key to staying ahead of the challenge of reducing the opportunities for threat groups to benefit from committing high-value cyber heists.



The role of the money-mule, in all of its guises can be seen as essential in

breaking the chain

between the initial fraud and laundering the stolen funds.



About BAE Systems Applied Intelligence

At BAE Systems Applied Intelligence, we help protect and enable organisations in the face of today's digital threats. With our track record for being the trusted partner of governments, we're uniquely placed to help financial services institutions counter economic crime and fraud.

We have a deep knowledge of the threat landscape and help over 200 financial institutions, including more than a third of the global top 100 banks, to mitigate risk. Our leading fraud and financial crime management solutions, combined with our experience and processes, help financial institutions play their role in foiling the criminal economy, while also embracing digital transformation.

We employ over 3,500 people across 17 countries in the Americas, APAC, UK and EMEA.

BAE Systems, Surrey Research Park,
Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/SWIFT

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

BAE SYSTEMS

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000