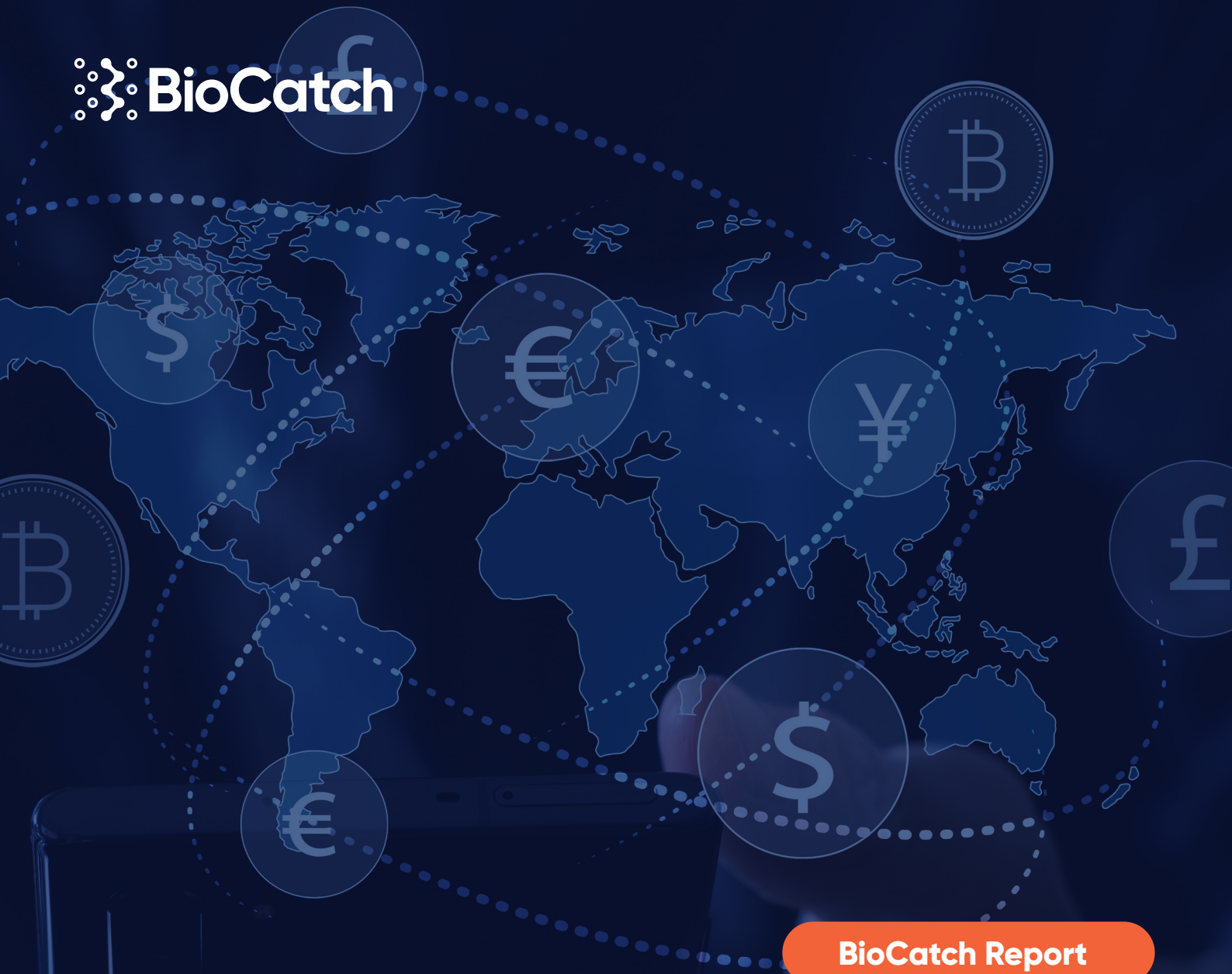
BioCatch



BioCatch Report

GLOBAL MONEY MULE NETWORKS

Using behavioral and device intelligence to shine a light on money laundering

Money mules: An overview

What are money mules?

Money mules are individuals who transfer, knowingly or unwittingly, money on behalf of others.

Why do they move money?

The funds moved by these money mules are the proceeds of criminal activity. By transferring these monies through a network of mule accounts, the money mules launder the funds so they can be re-integrated into the legitimate economy.

How do people become money mules?

There are different types of money mules, offering a variety of ways to become a money mule. For example, those responsible for these networks look to recruit people under the ruse of quick, easy money, with social media being commonly used to recruit complicit money mules. Other methods include manipulation, fraud and a variety of different scams to capture unwitting mules. For example, romance scam victims often inadvertently become money mules.

Who can be targeted to become a money mule?

Anyone. Typically, those suffering financial hardship are more likely to be recruited to be mules, but students are also considered a high-risk category.

Once recruited, what happens?

Money mules will be instructed to either open a new account for the sole purpose of washing stolen funds or to use a preexisting account for this laundering to avoid attracting the bank's attention.

What are the consequences of being a money mule?

Ultimately, money laundering is a crime, and as such, money mules are criminals prosecutable under the law. However, it is important to also consider that when moving money between accounts, money mules are indirectly involved in the crimes that produced the money they're moving (a diverse category that sometimes includes human, drug, and arms trafficking). Across the globe, there are laws that recognize money mules as accomplices to these crimes, leading to increased prison sentences.

Types of money mules

The five money mule personas

There are five main types of money mules identified by their unique characteristics and categorized by how complicit they are in a money laundering scheme.

THE DECEIVER

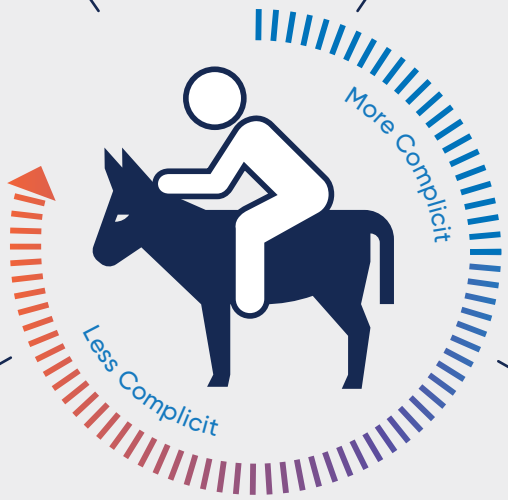
Opens new accounts using stolen or synthetic identities to send and receive stolen money. May sell access to these accounts to other fraudsters for a small fee. Likely to operate a network with hundreds or thousands of mule accounts.

THE VICTIM

Unaware that their account has been compromised and taken over by a fraudster to send and receive stolen money. Most likely their personal or account information was compromised in a data breach.

THE PEDDLER

Sells their genuine account to a fraudster who then uses it to send and receive stolen money. A common example of a Peddler is an international student who sells their account after completing their studies and returning to their home country.



THE MISLED

Sends and receives money on behalf of a fraudster believing the money is clean. A common example of this type of mule is someone who may have responded to a job advertisement that involves executing transactions on behalf of their "employer."

THE ACCOMPLICE

Opens a new account in their own name or uses an existing account to send and receive money at the direction of a fraudster. This money mule is a willing participant chasing an opportunity to make easy money.

Mules: The numbers

Almost 2 Million
bad accounts were identified and reported by BioCatch customers in 2024.

65% of money mules in the UK are younger than 30.[1]

71 months is the average sentence for money laundering offenses in the U.S.[2] In the UK, laundering charges can mean up to 14 years in prison.[3] In Australia, sentences ranges from 12 months to life.[4]

14% increase in money laundering cases in the U.S. between 2019 and 2023.[2]

$500 AU is all that money mules receive from Australian gangs in exchange for access to their bank accounts.[5] Some syndicates even offer $1000 to buy identity documents.[6]

1. https://www.gov.uk/government/news/biggest-ever-crackdown-on-money-mules-in-the-uk
2. https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY23.pdf
3. https://www.gov.uk/government/publications/money-mule-action-plan/money-mule-and-financial-exploitation-action-plan-accessible
4. https://www.austrac.gov.au/news-and-media/media-release/new-guidance-released-help-combat-use-foreign-students-money-mules
5. https://www.amlintelligence.com/2024/06/report-criminals-pay-australian-international-students-up-to-500-for-money-mule-accounts/
6. https://www.theguardian.com/australia-news/2024/nov/25/jackson-sold-his-id-to-an-australian-gambling-syndicate-hes-now-discovering-whats-been-done-in-his-name-ntwnfb

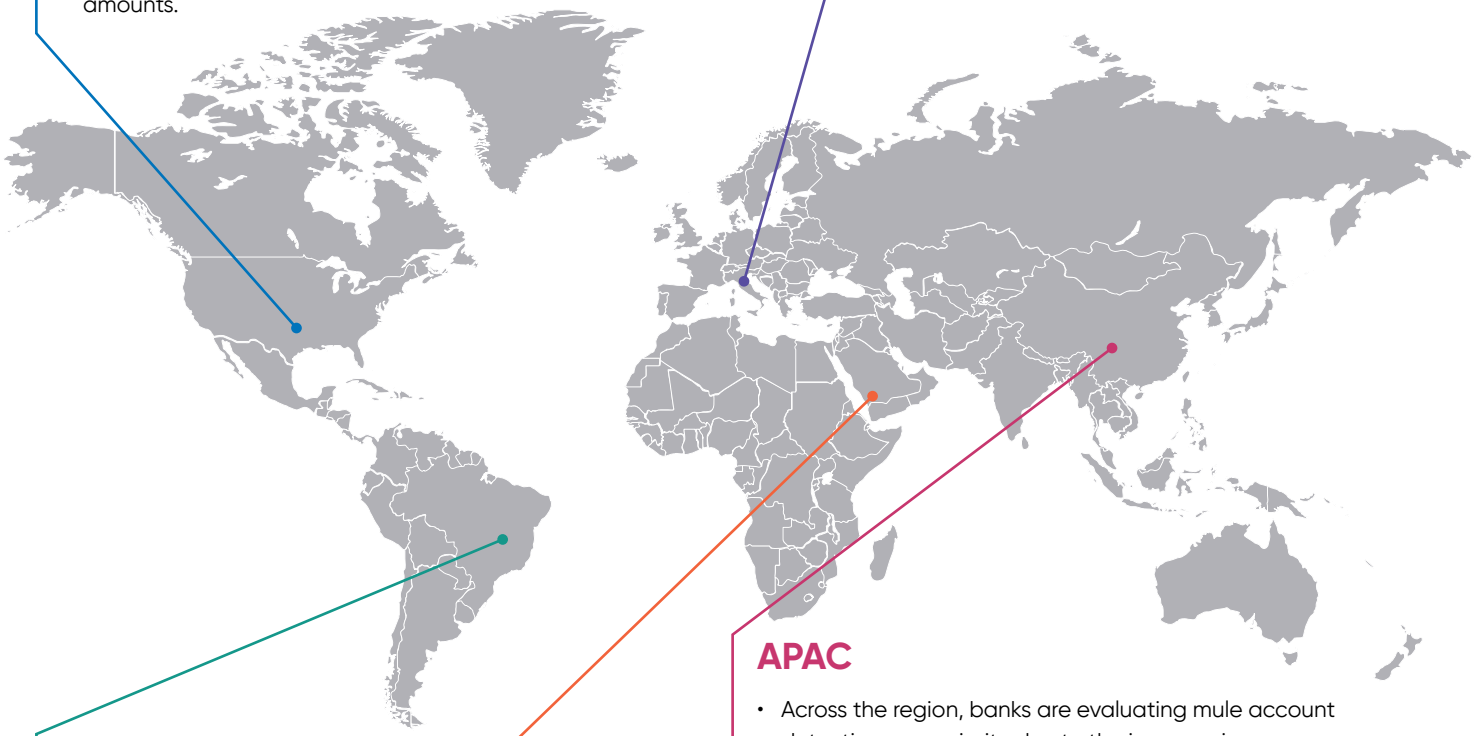
Global focus on mules

North America

- The increase in digital fraud and scams is leading banks to adopt new technologies to hunt down bad accounts.
- We've recently seen some high-profile fines for insufficient controls.
- Mule activity is usually seen on "drop accounts" that are opened specifically for mule activity, typically using true identities, which slip through banks' onboarding controls.
- Messaging apps and social media are the main methods used to recruit money mules, although email and SMS can also be used.
- Young people, particularly the 25-35 age group, are particularly vulnerable, lured in by the prospect of additional money from a side hustle.
- While a variety of payment methods are used to cash out the proceeds of mule activity, we typically see real-time payment services such as Zelle and Interac/EMT used for lower value payments, while wire and ACH transfers frequently handles higher amounts.

Europe

- Identifying mule accounts has recently become a focus for many banks across the region looking to get ahead of fraudsters and find different ways to tackle their fraud problems. Some banks are seeing a drop in the volume of mule accounts thanks to these efforts.
- PSR in the UK has accelerated the need for banks to identify bad accounts. Likewise, PSD3 in the European Union, has pushed for banks to explore ways to detect scams, with banks exploring the detection of bad destination accounts as a way to stop authorized frauds.
- Banks are seeing that mule accounts on their business portfolios are more common, given the tolerance for higher value payments.



APAC

- Across the region, banks are evaluating mule account detection as a priority due to the increase in scams.
- Australian banks have explored innovative ways to identify bad accounts, which has led to the creation of **BioCatch Trust**.
- There is encouraging collaboration between financial institutions, law enforcement and regulators in countries such as Australia, Singapore, and Hong Kong.
- Some countries have regulatory inconsistencies and significant resource limitations, which makes mule account detection challenging.
- Gambling is a focus area for money laundering detection region-wide, with unofficial sites and electronic gaming machines (colloquially known as "pokies" in Australia) causing significant concern.
- International students are a primary target of money mule networks in Australia, with AUSTRAC (Australia's anti-money laundering and counter-terrorism financing regulator) **issuing specific guidance** to help combat the exploitation of this subpopulation of the community.

Latin America

- Generally, there is a lack of regulatory sanctions for banks that have mule accounts, decentivizing the clean up.
- Countries, such as Brazil, are looking at ways banks can share data as a way of combating mule accounts. This could lead to more focus on detecting mule accounts in the coming years.

Middle East

- Efforts to modernize their banking sectors have led to efforts to strengthen AML regulations.
- Significant international cooperation among countries via the Gulf Cooperation Council (GCC) as well as the Financial Action Task Force (FATF).

SPOTLIGHT:

Money mules in the United Kingdom

Banks in the UK are reporting an increase in the number of money mules within their business portfolios. But why business accounts?

In the UK, one can register a new company for as little as £50, which is actually an increase from the £12 price tag we saw a few years ago. The process is also relatively easy, requiring little in the way of identity checks and scrutiny of background information. UK fraud leaders have referred to this process as "dysfunctional and facilitating fraud."[1]

Once a fraudster owns a legal entity in the UK, they can then start opening bank accounts, allowing bad actors – domestic and foreign – to access the UK financial system.

Fortunately, the Economic Crime and Transparency Act 2023 partially closed this loophole[2], taking steps to require more stringent identity checks. But gaps still exist, with business "owners" having a 12-month grace period to comply with the new ID requirements from the time their company is registered.[3]

Reports show that 168 companies registered in the UK have been identified as fraudulent.[4] While 168 may not sound like a lot, when we consider the amount of money that passes through each mule account – the National Crime Agency estimates that £10 billion is laundered through the UK banking system every year, and Cifas estimates 37,000 UK bank accounts exhibited mule-like behavior in 2023 – the potential financial impact is staggering.

£10 billion of illegal money is laundered each year in the UK.[5]

1. https://www.theguardian.com/business/2022/nov/08/companies-house-is-dysfunctional-and-facilitating-mps-told
2. https://www.gov.uk/government/news/companies-house-begins-phased-roll-out-of-new-powers-to-tackle-fraud
3. https://www.theguardian.com/business/2024/oct/18/companies-house-to-stop-fraudsters-signing-up-under-fake-names-like-darth-vader
4. https://www.thebureauinvestigates.com/stories/2023-01-29/sham-credibility-how-uk-shell-companies-fuel-pig-butchering-crypto-scams/
5. https://www.gov.uk/government/news/biggest-ever-crackdown-on-money-mules-in-the-uk

The evolution of mule account detection

In recent years, we've seen changes in how entities detect mule accounts and whose responsibility it is to do that detecting. While mule accounts traditionally fell under the remit of AML teams, typically waiting for the illicit activity to happen before action could be taken, other teams (such as fraud management groups) have begun exploring the possibility of proactive detection to disrupt mule networks.

There are many advantages of switching from defense to offense, but let's focus on two particular benefits. First, a proactive strategy makes it more difficult for fraudsters to execute fraud. With nowhere (or fewer accounts) through which to funnel money, life becomes harder for the bad guys. Second, we know proactive detection also reduces operational overhead – an increasingly vital need in this age of fraud: Nearly 70% of respondents to a Forrester survey reported an increase in the length of AML investigations in recent years.[1]

The importance of mule account detection

Detecting mule accounts is crucial for financial institutions – not only because legislation and regulation requires them to do so, but also because FIs have a moral duty to detect mules to protect the wider financial ecosystem. This in turn helps to protect their own reputations. Given that non-compliance can lead to significant penalties, it is also in their own financial interests.

The implementation of the latest rules imposed by the PSR (Payment Systems Regulator) in the UK, which regulates the reimbursement of authorized payment fraud, has introduced a new variable to this equation. With shared liability, receiving banks must now pay 50% of scam refunds. Therefore, harboring mule accounts, which fraudsters use to receive and then transfer away the proceeds of scams, will now cost banks money.

A similar liability shift has been seen in the U.S., although this has not been driven by regulation. With increasing pressure from lawmakers in the face of sharp increases in fraud numbers, Zelle, the major P2P payment network, has begun to take action and issue refunds to scam victims.

Compliance with regulations

As regulatory bodies across the globe have introduced regulation such as the European Union's Anti-Money Laundering Directive (AMLD) to hold banks accountable for preventing financial crime, the pressure on banks to comply with stringent rules has increased. This is seen in the number of fines placed on financial institutions in several geographies for non-compliance.

Mule accounts are often at the center of these cases, and authorities perceive the failure to detect and report these accounts to be due to insufficient AML controls. With this in mind, the detection of mule accounts could demonstrate a bank's commitment to complying with the law, not to mention protecting its customers from unwittingly being drawn into criminal schemes.

1. https://www.biocatch.com/improve-fraud-and-aml-operations

Protecting the financial ecosystem

Mule accounts play a key role in money laundering. More than 90% of all mule accounts identified in the European Union are linked to cybercrime. But criminals use mules to launder more than just the proceeds of online fraud.[2] Organized crime – drug traffickers, human traffickers, those who fund terrorism, and many others – also depends on mule accounts to fund and launder the proceeds of these heinous crimes.

By detecting mule accounts, banks can disrupt these operations, contributing to a cleaner economy, while protecting their customers.

As a reminder, there are three primary consequences of banks having mule accounts within their entity, which are summarized below. Therefore, it is in banks' interest to employ all their efforts into hunting out these accounts, and the earlier they can do so, the better.

90%

of all mule accounts identified in the European Union are linked to cybercrime.[2]

Reputational

Being associated with money laundering, even indirectly, can be damaging to a bank's brand image.

Regulatory

AML regulation is clear, and non-compliance can be very costly, bringing down significant fines.

Financial

Increasingly, regulation requires banks to reimburse fraud victims for their losses. There are also significant operational costs that come with detecting, investigating, and preventing mule accounts.

2. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

Dark ties between fraud, financial crime, and money laundering

Kevin Donovan,
SVP Emerging Solutions & Network

One of the major discoveries we uncovered while collaborating with financial institutions via our Mule Account Detection solution was how mule accounts connect fraud, financial crime, and money laundering.

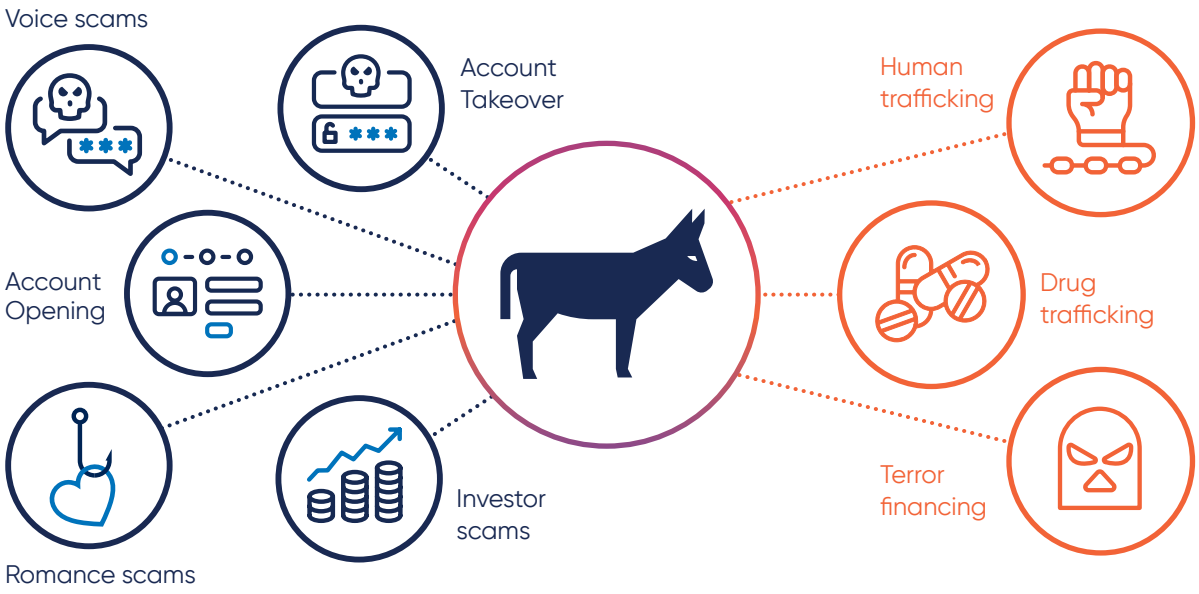
Historically, banks and vendors have separated fraud and financial crime detection, leading to significant silos within the bank and poor data sharing across different departments. But the reality is fraud, financial crime, and money laundering are all part of the same criminal ecosystem. Over time, as scams and mule networks increase in sophistication, we see the lines between these crimes blurring.

To offer some examples, **human trafficking operations used to conduct online scams have increased in recent years**. Likewise, many victims of investment scam fraud are actually acting as mules to launder money stolen via financial crime. These offer some insight into how the world of fraud and scams are linked to financial crime and money laundering, united under the umbrella of the dark economy.

In order to break this cycle, it is imperative to generate a wider understanding about the fundamental role mules play in support of financial crime operations and how interlinked fraud, money laundering, and financial crime truly are. According to NASDAQ's 2024 Global Financial Crime Report, $3.1 trillion in illicit funds were funneled through the global financial system in 2023.[1] Once we accept that every online fraudulent and financial crime scenario that moves money digitally requires a mule to execute that activity, we can anticipate and proactively disrupt these actions.

> "It is imperative to generate a wider understanding about the fundamental role that mules play in supporting a financial crime operation and how interlinked fraud, money laundering, and financial crime truly are."

The industry must adopt an innovative approach to financial crime management. Moving from reactive mule account detection (where banks identify mules after the laundered funds have already entered and then left the account) to proactive detection (where banks identify suspicious behavioral patterns before transactions even take place) can revolutionize mule account detection and, with it, fraud and scam prevention.



1. https://www.nasdaq.com/global-financial-crime-report

Case study

We know mule operators often act together as part of a wider criminal network. This leads to some interesting behavioral traits we can analyze to help detect mule accounts.

In the following example, we explore how BioCatch was able to alert one of its customers to a mule account, which was detected via behaviors suggesting the account was being accessed by multiple users.

Case context

- Account in question was opened and had no activity in its first four months of existence.
- There was steady activity over the following six months, with one low-value payment.
- After this period (at which point the account was almost a year old), we see a surge of activity, consisting of more frequent login activity, several payments and also a loan application. At this point, BioCatch provides an alert to the bank that this could be a mule account.
- Continued, high-intensity activity was ongoing for a further six months, with almost daily logins. Despite high suspicions, the bank was unable to determine for certain that the account was a mule.
- Upon receiving a significant inbound payment, the account was confirmed by the bank as a mule account.
- Account was opened by a graduate student (24 years old at the time of account opening).

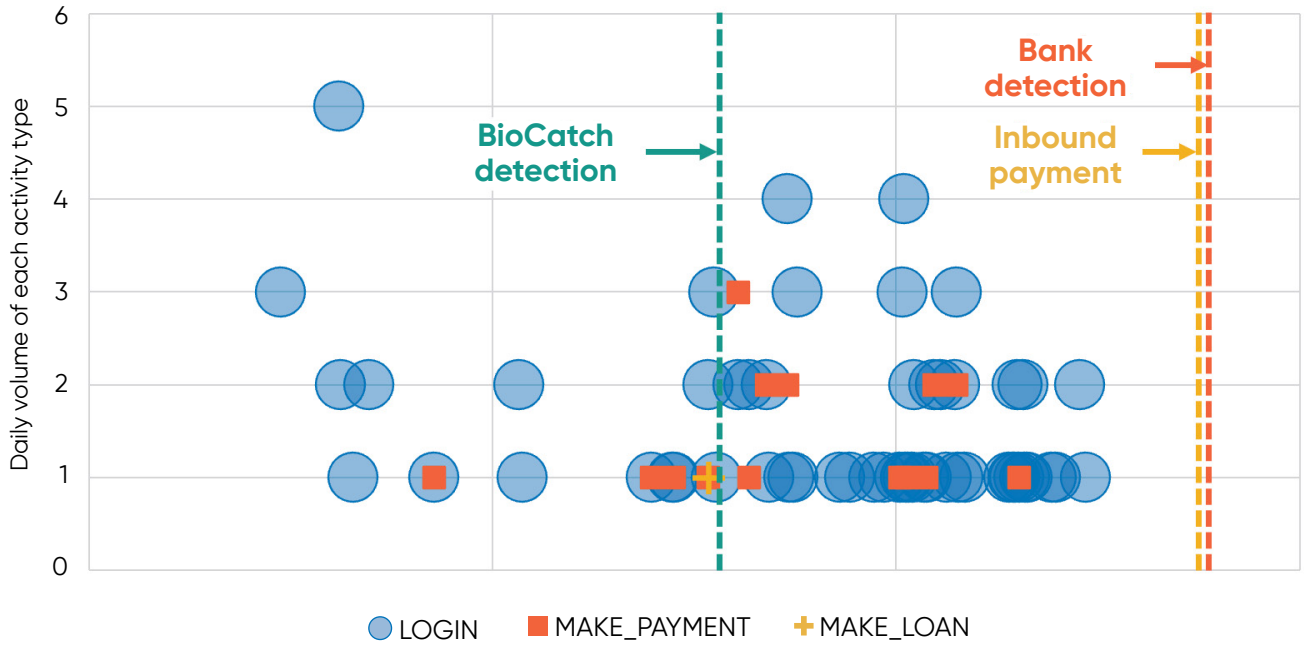
58%

of mules accounts see a **significant increase in login activity** synonymous with checking balances for inbound payments.

79%

of confirmed mule accounts were highly active 90 days prior to an incoming payment.

Timeline of user activity over account lifespan



Case study

Continuing with our analysis, we now look at how the user(s) interacts with the touch screen of their mobile device, using visualizations that show a reconstruction of all swipe and touch activity during mobile banking sessions.

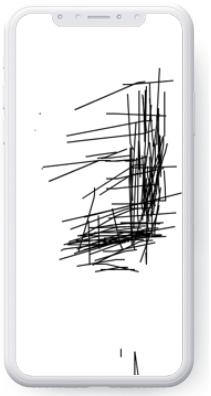
A comparative analysis allows us to draw conclusions that suggest not everything is normal, observing signs of a potential mule network operating the account.

The examples shown below are taken from six sessions that took place on three different devices. Across these sessions, we observe behaviors that suggest at least four potential users, due to the changes in cognitive behavior, including the hand dominance.

50 times

more likely to see users with **new device settings** in the mule population compared to the genuine population.

Chrome Mobile on Moto E5 Play
(Android 8.1)

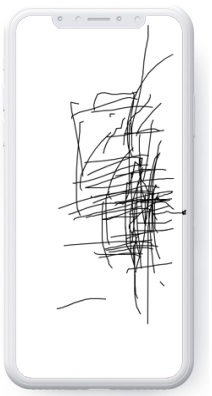


Righthanded
Standard usage and swipe patterns for mobile interaction
Potential user #1

Samsung Internet on Samsung SM-A217F
(Android)

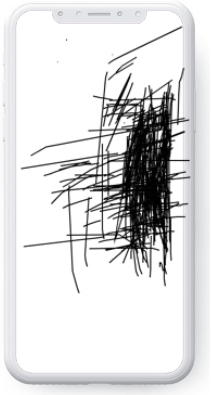
Both hands used; left hand preferred
New pattern on new device
Potential user #2

Mobile Safari on iPhone
(iOS 14)



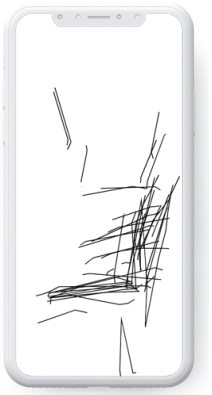
Righthanded
Normal usage consistent with a previous and rapid session
Potential user #3

Chrome Mobile on generic smartphone
(Android 6)



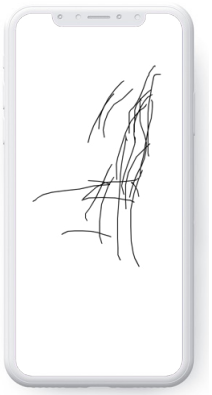
Righthanded
Swipe pattern consistent with Chrome sessions
Potential user #1

Samsung Internet on Samsung ISM-A217F
(Android)



Righthanded
New pattern but consistent device
Potential user #3

Mobile Safari on iPhone
(iOS 14)



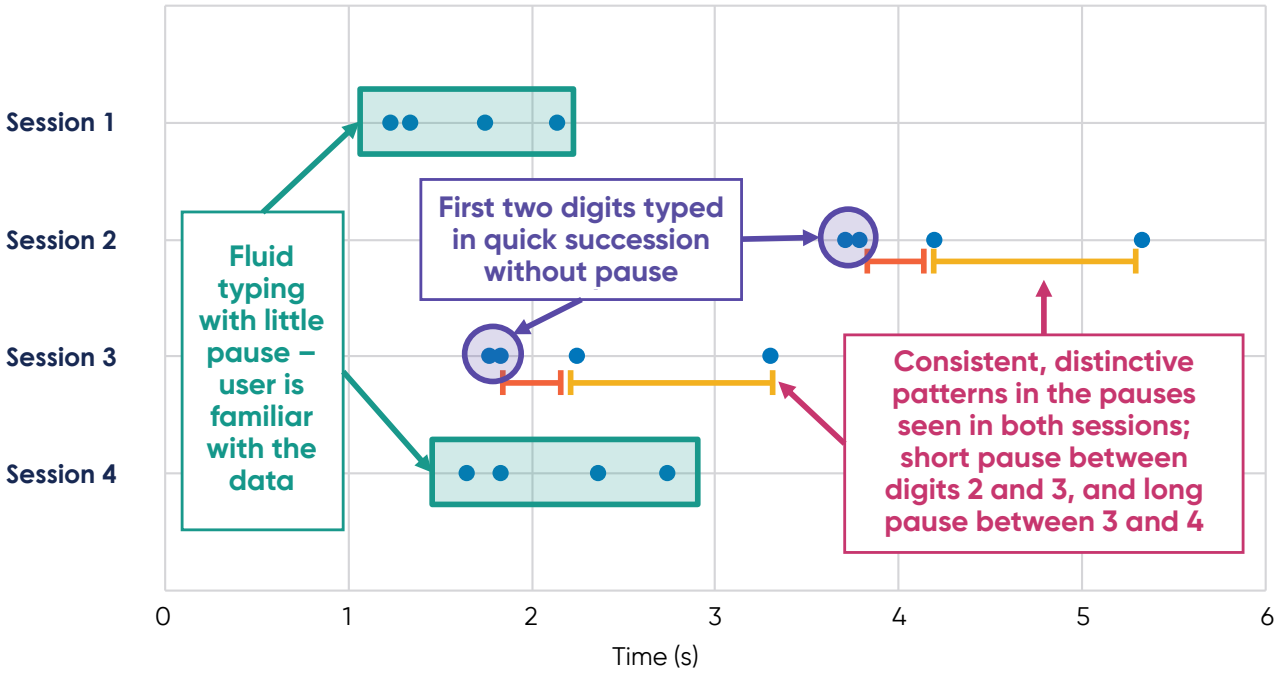
Righthanded
Swipe pattern different to other sessions with different curvature
Potential user #4

Case study

Our next area of analysis focuses on typing patterns.

Below we see a visual representation of how the user typed in their details during the login journey across four different sessions. In the graph, each dot represents a key stroke by the user, with the time calculated from when the user first clicked into the field. The greater the distance between two dots, the longer the user took to type each letter/digit.

For this bank, the field used to log in to digital banking is a section of a personal information field, i.e. date of birth, phone number, email address, etc. As such, there is an expectation that the user is familiar with this information and would have it as part of their long-term memory.



Typing analysis: Conclusions

- We see that there are distinctive patterns across the sessions that indicate (at least) two different users.
- Further analysis confirms that the different users identified here link back to the different users identified from the swipe patterns.
- The typing on sessions 1 and 4 suggest the user is familiar with the data – potentially their own data (considering this is a long-term memory field). Meanwhile, the typing on sessions 2 and 3 includes pauses that may suggest the user is consulting some sort of crib sheet that contains the data.
- Other sessions for this user include pasting of information during the login process. Not only does this introduce a third unique behavioral pattern, but it also reaffirms a level of unfamiliarity with personal data, suggesting multiple users operating the account.

Case study

Feature analysis

BioCatch models contain a set of behavioral features that offer insights to end users, assisting them with an increased understanding of model outcomes and providing them with binary data points that can be used for rule writing.

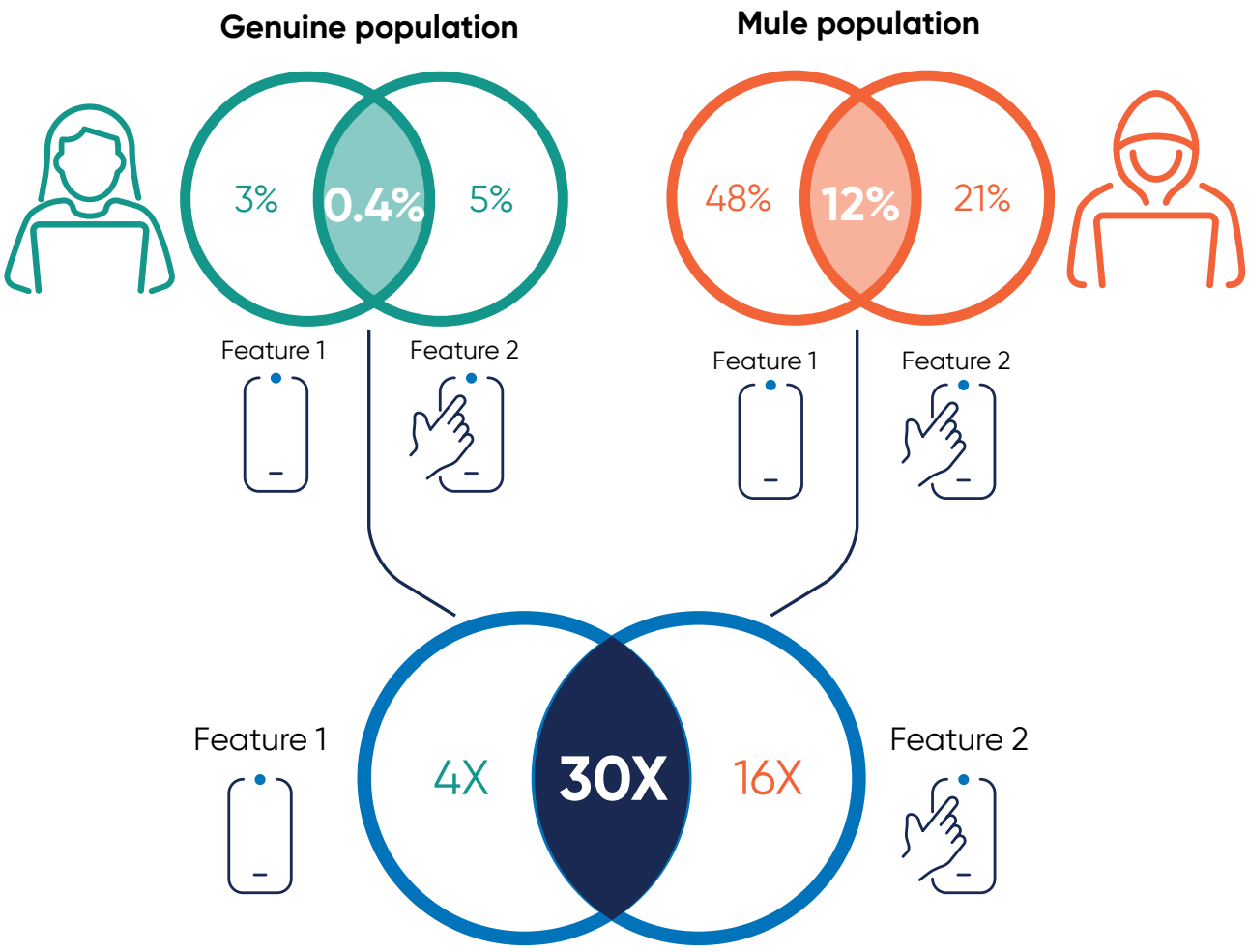
To conclude our analysis of this case, we have identified two features that were particularly useful in this case.

- Feature 1 – analyzes the user's device profile
- Feature 2 – analyzes the user's behavioral profile, specifically their cognitive preferences during the login process

In both cases, a "true" value alerts of anomalies that are inconsistent with the user profile.

When combining both features in a rule, we see promising results that set the base for effective detection when combined with additional information available to the bank.

30 times more likely to see this combination of features from confirmed money mules, compared to the general population.



Prevalence in mules vs genuine population

Case summary: What we've learned

We know mule accounts do not exist in isolation. They are often a part of a wider network of accounts, intertwined and managed for money laundering purposes. The ultimate goal for banks, together with law enforcement, is to shut down these networks.

At BioCatch, we have found network analysis to be an essential part of detecting mule accounts because it enables banks to trace and understand the complex relationships among accounts and users involved in fraudulent activities.

While identifying mule accounts is necessary, identifying and isolating individual accounts is often a futile exercise, given that these criminal organizations are able to replace downed accounts near immediately. Therefore, by identifying an account and evaluating the wider network to which it belongs, banks can shut down more total accounts and address the real problem: the criminal network behind the laundering.

This is why we introduced **BioCatch Scout**, a tool that empowers financial institutions with money laundering network data. Thanks to a visual representation of the connections between users, accounts, and devices, banks can see patterns that traditional transaction monitoring may miss. In many cases, this can also help with proactive detection, especially when illegally acquired funds have yet to enter a mule account.

To conclude, understanding the broader network enables banks to disrupt not just individual mule accounts, but entire criminal ecosystems, improving operational efficiency and protecting the institution from both reputational and financial risks.

BioCatch Scout is an investigational tool that analyzes and processes high-risk activity flagged by BioCatch's Account Takeover and Mule Account Detection solutions. It presents the information visually using network graphs.

The result is a galaxy of users, devices, and accounts represented in an intuitive way that allows investigators to drill down and examine relationships between users, often identifying connections and patterns that raw data alone (especially transactional data) cannot.

It also allows for reverse searching, allowing investigators to conduct detailed searches on specific users, devices, or accounts, or identify whether those users, devices, or accounts are connected to high-risk networks. Likewise, its integration with existing BioCatch tools, primarily Analyst Station, offers investigators wide-reaching historical data on previous sessions, as well as all previous fraud feedback.

In many cases, this helps with proactive detection, particularly where funds have yet to hit an account.

Screenshot taken from BioCatch Scout showing a part of the galaxy for one financial institution.

An example of one of these galaxy network graphs (this one at a U.S. credit union) is shown above.

By leveraging BioCatch Scout, this institution was able to uncover 10 distinct devices that were accessing three newly created accounts. This allowed them to intercept $43,000 in fraudulent ACH transfers before the criminals could move the funds elsewhere. Furthermore, they identified an attempted identity theft when one of the fraudsters tried to secure a $5,000 credit line. By detecting these fraudulent activities early, the credit union successfully safeguarded its customers and avoided significant financial losses.

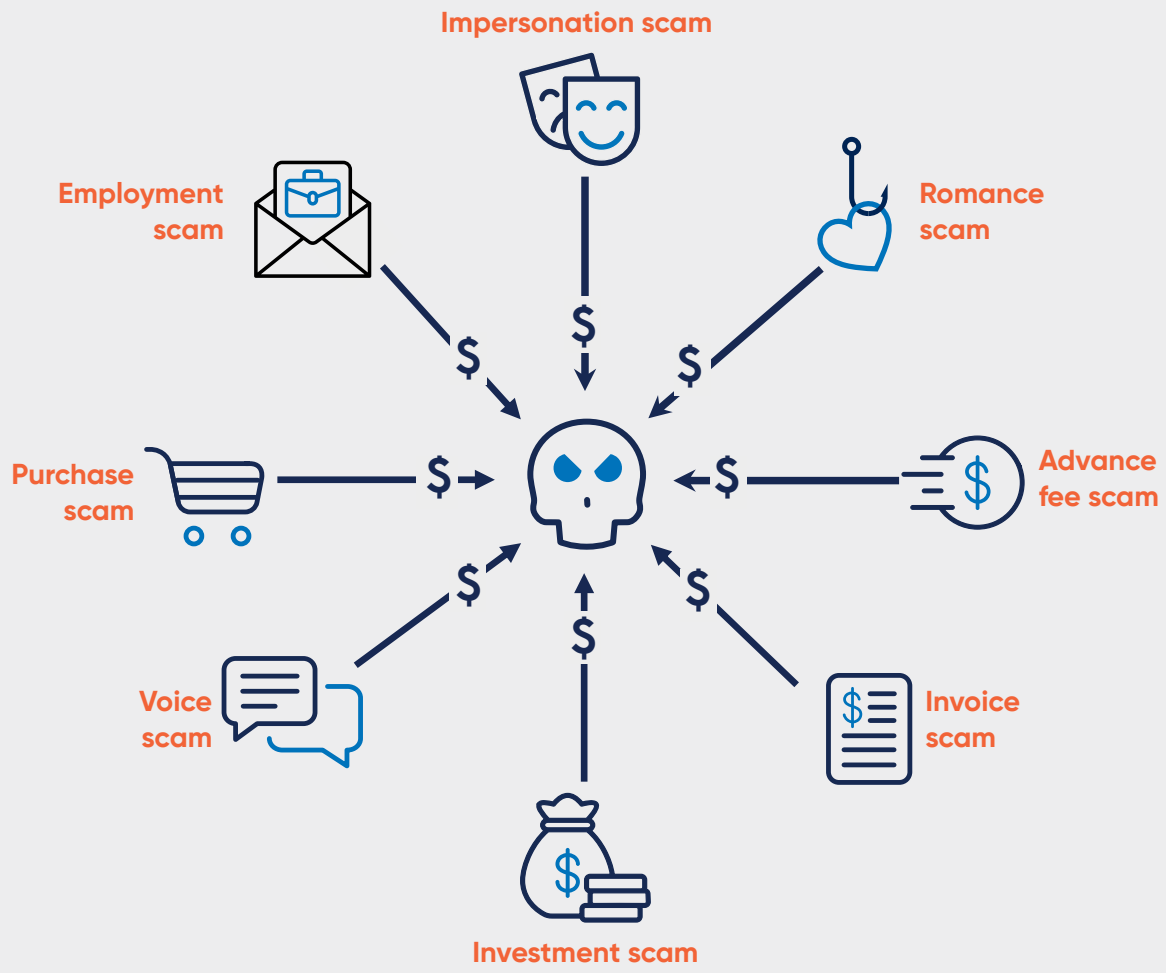
In summary, BioCatch Scout offers banks a tool that aids in investigations, thus increasing operational efficiency and improving fraud detection both within and across different bank teams.

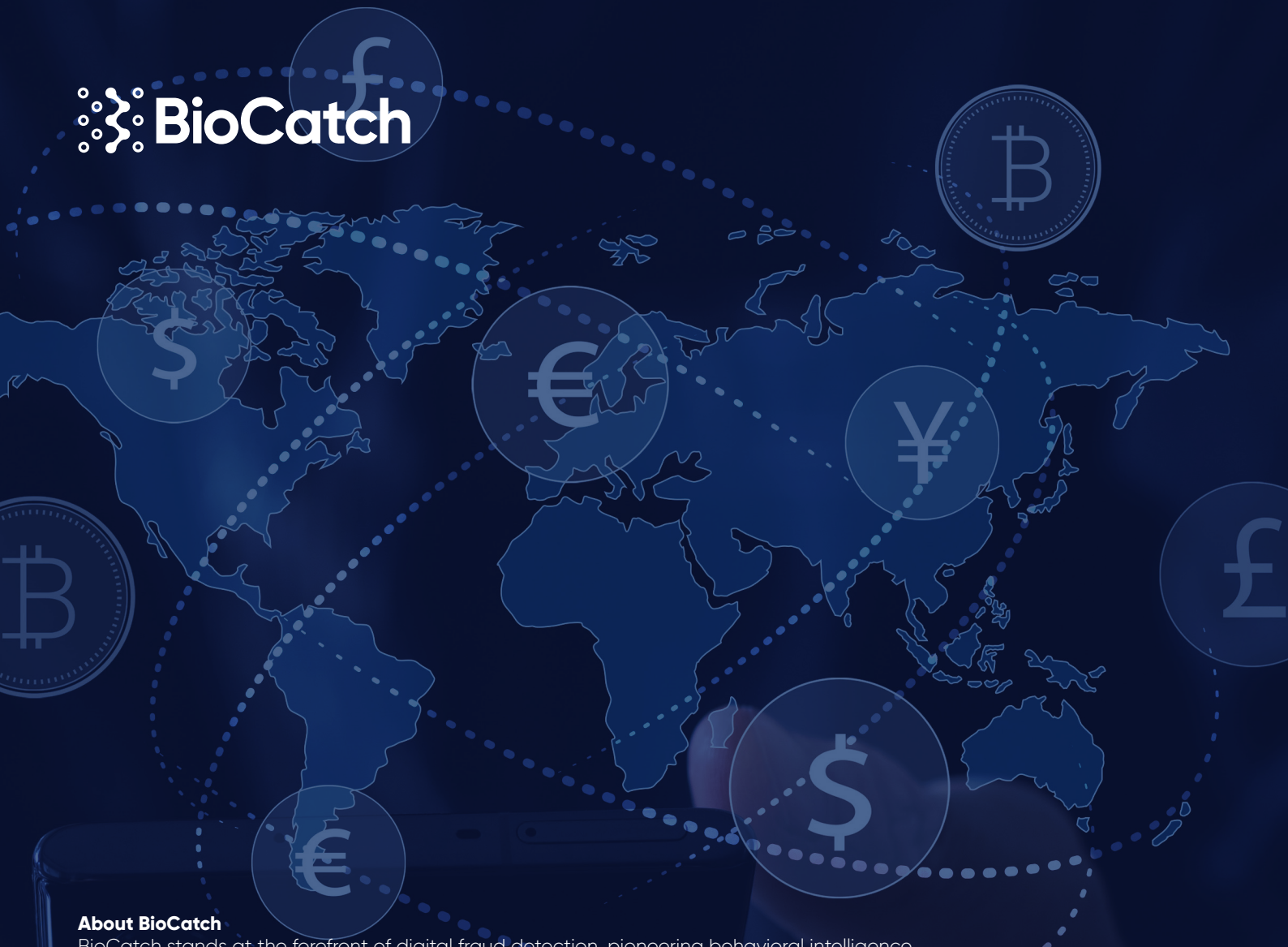
All scams lead to mules

At BioCatch, we believe the early detection of mule accounts is crucial to controlling the scam epidemic. Ultimately, all scams lead to mules. Eliminating mule accounts impedes the fraudster's ability to extract their stolen money, making scamming it in the first place a more futile exercise.

We know that in some geographies, consumer protection rules make it difficult for financial institutions to shut down suspected mule accounts, especially if illicit funds have yet to hit the account. But even when these accounts remain open, banks can still leverage mule account intelligence to keep their customers safe.

BioCatch Trust, for example, uses account-level intelligence on the receiving end of payments to assess the risk of a payment, so even if consumer protections prevent the bank from closing a mule account, by flagging that account as a mule, fraud teams can halt any transactions directing money to the account, thereby preventing their legitimate customers from falling victim to scams.





About BioCatch

BioCatch stands at the forefront of digital fraud detection, pioneering behavioral intelligence grounded in advanced cognitive science and machine learning. BioCatch analyzes thousands of user interactions to support a digital banking environment where identity, trust, and ease coexist. Today, 34 of the world's largest 100 banks and 237 total financial institutions rely on BioCatch Connect™ to combat fraud, facilitate digital transformation, and grow customer relationships. BioCatch's Client Innovation Board – an industry-led initiative featuring American Express, Barclays, Citi Ventures, HSBC, and National Australia Bank – collaborates to pioneer creative and innovative ways to leverage customer relationships for fraud prevention. With more than a decade of data analysis, 93 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges. For more information, please visit **www.biocatch.com**.

www.biocatch.com **E:** info@biocatch.com @biocatch **in** /company/biocatch

Tel Aviv | New York | Boston | London | São Paulo | Santiago | Mexico City | Melbourne | Mumbai | Singapore