Issue 112 | March 2026

NTT DATA

Radar

The cybersecurity magazine

Breaking the Fraud Chain: The Key Role of Money Mules

By Miguel Angel Soler Barba and Alejandra Romero Gutiérrez

Financial fraud has become one of the major global challenges of our time. Its sustained growth is not constrained by borders: it affects banks, companies, businesses, public institutions, and citizens across all continents. Increasingly sophisticated investment scams, large-scale identity impersonation, payment fraud, and social engineering attacks now converge within a criminal ecosystem that operates on an international scale. In this context, one common factor remains decisive for offenders' success: money mules.

Money mules—individuals who move illicit funds through their accounts, sometimes deceived and at other times acting voluntarily—have become the essential infrastructure of modern fraud. Without them, fraudsters would be unable to convert their proceeds into usable money or to conceal their trail through multiple transfers across different jurisdictions. The global nature of the digitised financial system has multiplied both opportunities and risks, making the fight against money mules a transnational challenge.

The regulatory landscape is evolving to address this threat. International bodies such as the FATF (GAFI), new European authorities such as AMLA, and frameworks such as PSD2/PSR, DORA, NIS2, the forthcoming global standard for instant payments, and the Digital Euro Package are imposing stricter requirements for identity verification, transaction monitoring, and the management of operational and cyber risk. Regulation is no longer focused solely on procedural compliance; it increasingly demands demonstrable effectiveness in fraud prevention, including the detection and disruption of mule networks.

Cybersecurity, for its part, has become an inseparable pillar of the fight against fraud. Today's attacks combine malware, phishing, spoofing, session hijacking, and large-scale psychological manipulation. Collaboration between fraud teams and security operations centres (SOCs) is now indispensable to correlate technical and financial signals using cyber threat intelligence. Money mules are the ultimate destination of many of these attacks, which has tightened the link between cyber threats and transactional fraud more than ever before.

The complexity and speed of mule networks make a response based solely on static rules or manual reviews unworkable. Advanced analytics, at varying levels of maturity, has become the primary ally in anticipating, detecting, and dismantling these networks.

Through dashboards and exploratory analyses, organisations can identify fraud typologies, concentrations by channel or product, and examine the life cycle of mule accounts. Statistical and machine-learning models make it possible to estimate the likelihood that an account is acting as a mule, as well as to detect anomalous behaviour and analyse network patterns.

Moreover, the combination of risk scores, dynamic rules, and simulations is enabling organisations to recommend optimal actions, prioritise investigations, and balance fraud risk, cost, and customer experience. All of this makes continuous learning essential—and this is where AI plays a central role: learning continuously, detecting weak signals and complex combinations invisible to traditional rule-based approaches, analysing entire networks, and scaling detection across millions of transactions and relationships.

When generative AI is added to the equation, it introduces a qualitative shift in the fight against mule networks by focusing on amplifying the capabilities of human teams.

The technological horizon extends even further. Quantum computing, while still in its early stages, presents both challenges and opportunities: on the one hand, it could in the future undermine current encryption methods; on the other, it promises unprecedented analytical capabilities to trace complex relationships among thousands of accounts and transactions. Preparing for a "post-quantum" world will be essential to maintain the resilience of the financial ecosystem.

From a strategic perspective, this reality underscores a key message for the sector: without a comprehensive and integrated view of fraud in general—and of the money-mule phenomenon in particular—effective prevention will not be possible. Mule networks evolve rapidly, adapting to existing controls, and can only be contained through agile operations, stringent oversight, and analytical capabilities able to learn, anticipate, and continuously recalibrate.

The fight against money mules ceases to be a purely operational problem and becomes a structural decision about how risk is governed in the digital era.

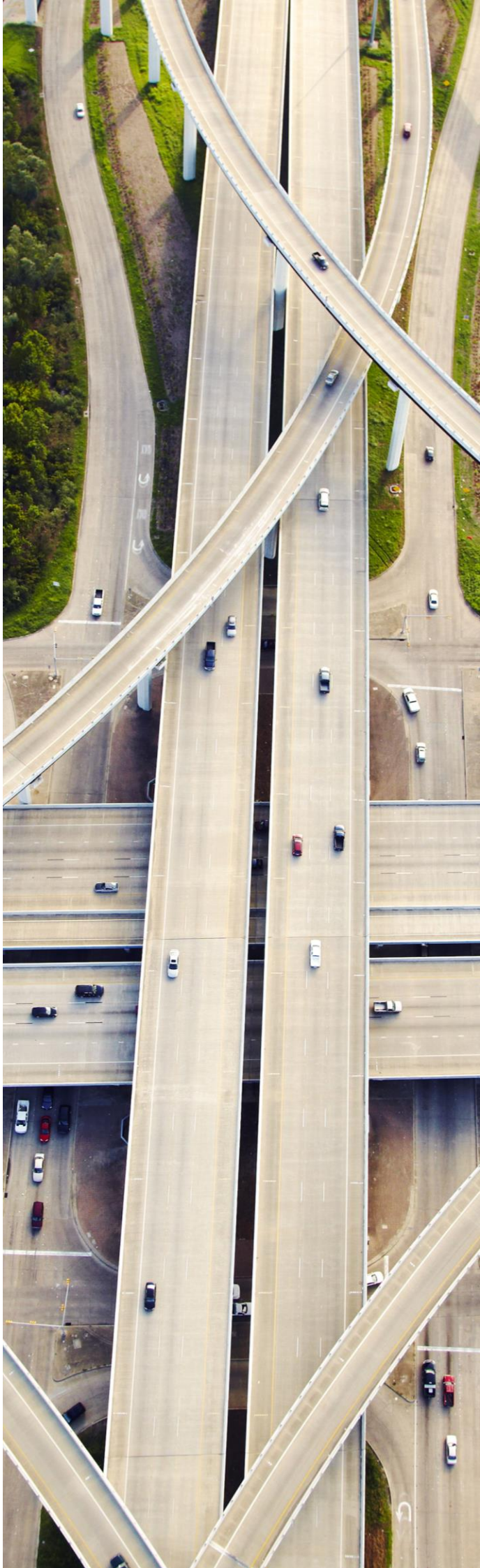
Ultimately, the issue of money mules is far more than an operational matter: it is a global challenge that requires smart regulation (without unduly constraining citizens' legitimate activity), technology that integrates fraud prevention and cybersecurity, advanced analytics, and cross-border collaboration. If we succeed in weakening this critical link, we can significantly reduce fraud and safeguard the trust on which the global financial system depends.

Throughout this issue of our publication, *Radar*, we will explore in depth how financial institutions manage the detection and mitigation of mule accounts across their life cycle. The process is divided into three critical stages: customer onboarding, the latency period, and real-time transaction monitoring. We will highlight the technological evolution driven by proactive and reactive machine-learning models that enable suspicious patterns to be identified with greater precision.

In addition, we will examine how artificial intelligence tools facilitate both the creation of fraudulent identities by criminals and their detection by banks. Finally, the paper will reflect on the future implementation of agent-based systems to automate alert analysis and improve operational efficiency.

Miguel Angel Soler Barba
FinCrime Manager

Alejandra Romero Gutiérrez
Fraud Prevention Manager



Attacks on European Institutions

Cyber Chronicle by Leire Cubo Arce

The first months of 2026 have confirmed that the cybersecurity landscape remains under strain and is evolving continuously. Over the past month, significant incidents have been reported affecting European public institutions, major international events, and strategic sectors, while consolidated reports indicate sustained growth in ransomware and digital fraud.

One of the most significant episodes occurred within the European institutional sphere. At the end of January, the European Commission confirmed an unauthorised access to its corporate mobile device management (MDM) platform. The incident, detected and contained in less than nine hours, enabled attackers to access limited personal data belonging to certain officials, including names and professional telephone numbers.

Although the mobile devices managed by the platform were not directly compromised, authorities warned of the risk that the extracted information could be used in highly targeted phishing campaigns against institutional staff. The case once again highlights the exposure of critical internal management tools, which are increasingly attractive targets for advanced threat actors.

At the same time, geopolitical tensions once again spilled over into cyberspace. In the weeks preceding the Winter Olympic Games in Italy, the Italian National Cybersecurity Agency confirmed coordinated attempts to launch distributed denial-of-service (DDoS) attacks against official event portals and infrastructures linked to the tourism and logistics environment in Cortina d'Ampezzo.

The actions, attributed to a pro-Russian hacktivist group, aimed to generate disruption and media visibility during a high-profile international event. The mitigation measures deployed successfully neutralised the malicious traffic without causing significant service outages; however, the episode confirms that major global events continue to serve as symbolic targets within the broader context of digital confrontation.

At the national level, the most recent data reflect a considerable increase in criminal activity. The National Cybersecurity Institute (Incibe) reported that more than 122,000 incidents were managed during 2025, representing a 26% increase compared with the previous year. Particularly noteworthy is the 171% growth in cases involving digital information theft, as well as the persistence of thousands of phishing and online fraud campaigns. In addition, more than 400 incidents affected operators classified as essential, including sectors such as banking, transport, and energy. These figures demonstrate that the threat is not only becoming more frequent, but also directly impacting critical infrastructure and strategic services.

Ransomware, for its part, continues to exhibit a high global incidence. Sector reports for January 2026 indicate attack volumes above the historical average, with particularly significant impact on healthcare, governmental, and industrial organisations. Criminal groups continue to refine double-extortion models, combining system encryption with threats to publish exfiltrated data. The increasing professionalisation of these criminal structures, along with the diversification of their access vectors—frequently through compromised credentials or vulnerabilities in exposed services—further complicates early containment efforts.

At the same time, experts have warned of the large-scale exploitation of connected household devices, particularly smart televisions and Android-based streaming systems. These devices, often misconfigured or lacking security updates, are being recruited into botnets used to conduct distributed denial-of-service (DDoS) attacks. This trend demonstrates that the attack surface is no longer confined to the traditional corporate perimeter; rather, it extends into the digital ecosystem of the connected home, which may unknowingly become infrastructure serving the attacker.

Taken together, developments over the past month depict a landscape in which cybercriminal activity combines political motivations, financial gain, and the systematic exploitation of technical vulnerabilities. Rapid detection, coordinated response capabilities, and effective technology lifecycle management are consolidating as key elements in reducing impact. The beginning of 2026 thus confirms that cybersecurity remains an essential strategic component for institutional, economic, and social stability in an increasingly interconnected environment.

Leire Cubo Arce
Cybersecurity Engineer

Money Mules: Reconsidering the Relationship Between AML and Fraud

Article by José Frías Hernando

Over the past decade, nearly every aspect of financial activity has changed almost overnight. Customers now operate seamlessly across digital and non-digital channels with a level of ease that would have seemed impossible just a few years ago, and organisations have had to adapt their models to a far more digitally driven relationship. Yet amid this transformation, an uncomfortable reality has emerged: financial crime has evolved as well. It has done so quietly, exploiting gaps in the system and, in many cases, moving faster than the controls designed to contain it.

Added to this reality is a fundamental asymmetry: while financial institutions operate under increasingly stringent regulatory frameworks—complying with obligations related to AML (anti-money laundering), consumer protection, privacy, governance, and operational resilience—cybercriminals are subject to none of these constraints. They are not required to balance innovation with compliance, nor speed with control; this absence of obligations grants them an agility that, in practice, translates into a structural advantage over organisations that must protect their customers while remaining fully compliant with regulation.

Yet one of the most concerning developments for supervisors in this new landscape is the growth and diversification of money mules. For a long time, the sector assumed that a mule fit the classic profile of an individual who lent their account in exchange for some financial compensation or an attractive return—an actor acting in apparent good faith, yet generally aware of their involvement. Today, that caricature no longer holds.

Institutions are now confronted with students lured by offers that appear harmless, workers seeking additional income without realising they are being exploited, victims of identity theft, and, increasingly, synthetic identities that bypass initial controls through ever more sophisticated techniques.

This scenario not only complicates detection but also reshapes risk perception and compels institutions to reassess how protection is defined and implemented from the very outset of the customer relationship.

A Problem That Has Moved to the Centre of the Regulatory Agenda

This phenomenon is not new; regulators had already incorporated it into their roadmaps long before it reached media headlines. The issue of money mules is far from anecdotal for supervisory authorities.

It is also regarded as a symptom: when an institution allows its products to be used to move illicit funds—even where the customer has been deceived—it may reveal weaknesses in onboarding policies, the institution's capacity to conduct regular analytical reviews, or the integrity of its risk models.

Over time, supervisors have increased their expectations. Identity verification and record-keeping alone are no longer sufficient. Authorities now seek a comprehensive understanding of what institutions are doing to assess whether customer behaviour is consistent with their profile, whether inconsistencies emerge in early activity, whether customers may be subject to manipulation practices, or whether their transactional patterns are already linked to known criminal networks.

Onboarding, therefore, is no longer merely a validation stage; it has become a first line of defence in ensuring the quality and sustainability of an institution's growth.

Another significant shift concerns accountability. While a mule may indeed be a victim, regulators do not consider this fact to constitute a safeguard for the institution as a whole.

The expectation is clear: banks must be able to demonstrate that they have designed and implemented control frameworks robust enough to effectively identify abnormal behaviour before it escalates into operational or reputational risk.

AML and Fraud: Two Worlds That Were Always Connected, but Must Now Be Formally Integrated

If anything has facilitated the rise of money mules, it is the operational distance that has long existed between anti-money laundering (AML) teams and fraud prevention teams. Both observed complementary signals, yet these were rarely incorporated into a single, unified view.

AML focused on flows, income consistency, and the origin of funds. Fraud teams assessed transactions—including outgoing payments—devices, access patterns, transaction velocity, and execution behaviour. Each function generated alerts according to its own logic, without constructing a comprehensive narrative around the customer. This fragmented approach is no longer sustainable. Money mules operate precisely at the intersection of these two domains, and if the pieces are not connected, the risk can evade detection.

The most proactive institutions have recognised this shift. Those adapting to the new reality advocate for AML and fraud functions to operate jointly, developing shared models and integrating data, criteria, and decision-making processes. This requires not only a transformation of governance structures, but also of workflows: unified case management, joint analytical frameworks, integrated risk scoring, and—above all—a holistic interpretation of customer behaviour that considers not only what the customer does, but how they do it and the apparent intent underlying their actions.

The result is a broader and more coherent perspective. Rather than interpreting disconnected signals, the institution views the customer as a dynamic and evolving entity, enabling earlier and more decisive intervention with broader risk implications.

The Role of the Business: Growth, Yes—but with a Different Understanding of Risk

The business function is deeply affected by these regulatory and operational developments. Customer acquisition can no longer be assessed solely on numerical growth. Volume alone is no longer sufficient.

Instead, many institutions are increasingly pursuing what is often described as “clean growth”: growth that does not erode behavioural quality, generate excessive alerts, or ultimately become a source of risk for the organisation.

When growth disregards this risk dimension, the impact extends beyond internal or regulatory metrics: it translates into customers who feel unprotected and who—even without suffering a direct financial loss—reduce their level of trust, limit their engagement with the institution, and erode key opportunities for loyalty and cross-selling.

One of the first outcomes of this shift in mindset is a change in admission policies. Institutions are incorporating less visible yet more meaningful filters, based on early risk indicators derived from both AML and fraud perspectives.

This does not necessarily imply making the process more restrictive; rather, it entails applying greater flexibility where risk is absent and greater scrutiny where evidence points to vulnerability or exposure to manipulation.

Business Adaptation: Evolving Policies, Risk-Aware Customer Journeys, and a New Balance Between Growth and Quality

At the same time, customer journeys are being redesigned. They are no longer viewed as linear pathways aimed solely at maximising conversion. Instead, more sophisticated control points, preventive messaging, and, in some cases, dynamic restrictions are being integrated and activated when customer behaviour deviates from expected patterns.

Far from undermining the user experience, this strategy fosters a safer digital environment and greater awareness of emerging threats.

Internal metrics are also evolving. Conversion is becoming qualified conversion; customer value is being assessed using criteria that were not even considered a few years ago. Even commercial incentives are beginning to shift, encouraging growth that no longer rewards business segments which, in the long term, generate higher operational friction and increased regulatory exposure.

Conclusion: A Challenge That Redefines What It Means to Do Business in the Financial Sector

Money mules are neither a passing trend nor a statistical anomaly. They represent a form of financial crime that has grown in complexity and systematically exploits vulnerabilities within the underlying system.

Their scale has compelled the sector to accelerate changes that had already been underway: greater harmonisation between AML and fraud practices; more adaptive policies; more deliberate and risk-aware customer journeys; and a risk mindset that monitors customers throughout their entire lifecycle.

Regulators have set the direction, but it is ultimately up to institutions themselves to recognise that sustainable growth depends on their ability to detect and contain this threat effectively.

Those institutions that successfully integrate this approach will not only be better positioned to meet regulatory expectations, build customer trust, and develop more resilient business models; they will also strengthen the credibility and robustness of their operations in an increasingly fast-moving environment where financial crime continues to expand within a more uncertain global landscape than ever before.

José Frías Hernando
Head of Anti-Money Laundering

Technological Evolution of Fraud Prevention Tools

Article by Francisco José García Spina

Financial fraud has entered a radically different phase. Money mules and advanced scams are no longer isolated incidents; they have become coordinated threats capable of impacting multiple institutions simultaneously. The combination of instant payments, open fintech ecosystems, and vulnerable digital identities has expanded the risk perimeter and compelled the financial sector to evolve its anti-fraud technology stack faster than ever before.

In this context, the challenge is no longer merely to identify an anomalous transaction, but to disrupt entire networks—dynamic and distributed—that continuously adapt in order to evade controls.

For years, prevention tools relied on static rules and controls designed for a more stable digital ecosystem. That approach has now been overtaken. Contemporary fraud is characterised by sophisticated social engineering, direct user manipulation, identity impersonation, the use of synthetic identities, and mule networks executing rapid patterns of placement, layering, and dispersion. To respond effectively, modern tools must go beyond transactional analysis and develop a contextual understanding of what a customer does, how it is done, from which device, under which digital signals, and within what network of relationships.

This transformation is giving rise to a new generation of platforms incorporating advanced artificial intelligence, graph analytics, behavioural biometrics, intelligent orchestration, and architectures capable of anticipating suspicious behaviour in real time.

Within this framework, advanced analytics has become the core of the modern anti-fraud model. Descriptive analytics enables institutions to understand the true scale of the money mule phenomenon and to prioritise efforts accordingly. Predictive and machine-learning models anticipate risk by identifying anomalous behaviour and network patterns. Prescriptive analytics translates that risk into actionable decisions, balancing financial impact, customer experience, and regulatory compliance.

Artificial intelligence further contributes continuous learning and scalability, enabling sustained anti-fraud effectiveness in the face of constantly evolving criminal tactics.

Generative AI complements this approach by acting as an operational accelerator: it analyses unstructured information, assists analysts in investigating complex cases, and enhances the explainability of decisions. It does not replace human judgement; rather, it amplifies human capability and efficiency.

Understanding the Mule Lifecycle: The Starting Point of the New Approach

The traditional mule cycle, placement and layering, remains conceptually valid, but today it unfolds at a speed that overwhelms conventional models. The natural evolution has therefore been a shift from reactive AML monitoring to a proactive, technology-driven approach that integrates:

- Advanced controls in digital onboarding and early risk assessment
- Intelligent alerts generated by AI models
- Relationship identification through graph analytics
- Contextual analysis based on channel, device, and transaction velocity

This relational model enables the detection not only of a suspicious user, but of the entire cluster to which that user belongs.

Agentic AI: The New Operational Muscle of Anti-Fraud

One of the most significant innovations is the emergence of specialised AI agents that automate critical stages of the fraud lifecycle and make decisions within milliseconds:

- **Secure Onboarding Agent:** identifies synthetic accounts, repeated device usage, and indicators of “account factories.”
- **Activation and Dispersion Agent:** monitors rapid pass-through transactions and recommends preventive holds.
- **Orchestration Agent:** combines rules, models, and risk appetite parameters to determine whether to approve, escalate, or block a transaction.

These agents enable institutions to operate at the speed of modern fraud, where rapid response is decisive.

Modern Architectures: From Transactional to Relational

Today's tools no longer operate as standalone engines; rather, they function as integrated anti-fraud ecosystems that combine multiple layers of intelligence and control. These include:

- Graph analytics to detect risk clusters and uncover hidden relationships.
- Hybrid models (rules + AI) designed to reduce false positives while maintaining high detection accuracy.
- Advanced digital signals, such as behavioural biometrics, IP intelligence, and Remote Access Trojan (RAT) detection.
- End-to-end traceability through enhanced logging capabilities and, in certain cases, blockchain-based mechanisms.

The result is more precise and contextual detection, capable of anticipating patterns of human or automated manipulation rather than merely reacting to isolated anomalous transactions.

The Future: Interbank Collaboration and *Federated Learning*

The next evolutionary leap lies in collaborative detection across institutions. Through federated learning, banks can share intelligence without exposing sensitive data. This approach makes it possible to:

- Detect money mules operating across multiple institutions.
- Identify repeated devices or identities within the broader ecosystem.
- Anticipate criminal campaigns before they scale and propagate.

Conclusion

The financial sector is undergoing a structural transformation in its fight against fraud. Static rules are no longer sufficient. Modern tools incorporate artificial intelligence, graph analytics, advanced digital signals, and intelligent architectures capable of dismantling entire networks and anticipating attacks.

The mission is no longer limited to stopping fraudulent transactions; it is to understand the network, anticipate risk, and act before fraud materialises.

Francisco José García Spina
Head of FinCrime Solutions

Operational Impact of Money Mules

Article by Carlos Campos Hervas

From an operational perspective, once preventive mechanisms have failed to block their entry, the management of money mules focuses on detecting them as early as possible in order to prevent their activity, identify other potential mules, and subsequently terminate the relationship (account closure and customer offboarding, among other measures). A mule can be detected at three key stages of its "lifecycle": onboarding, latency, and transaction activity.

On-boarding

From an operational standpoint, onboarding consists of verifying the customer's identity, documentation, and related data. Except in very clear cases, such as the use of the same mobile device or address by multiple individuals, irregularities in documentation, or alerts triggered during identity verification (photo/video checks), it is extremely challenging to identify a money mule at the entry stage. As a result, specific models are being developed to address this gap.

Identity verification is the area where tools are advancing most rapidly, enabling more accurate detection of replicated faces or faces already present in databases of known illegitimate individuals. At the same time, however, AI-based tools allow criminals to generate synthetic images with increasing precision and speed. There have been cases involving individuals making hundreds of onboarding attempts using different faces or identification documents. Consequently, improvements in detection are often offset by parallel advances in the generation of false identities.

AML (Anti-Money Laundering) control processes, such as KYC (Know Your Customer), also provide limited additional insight for early mule detection, as many individuals register under profiles such as students or homemakers—categories that typically require minimal supporting documentation.

Latency

It is during the active life of mule accounts, through analysis of account activity, that detection becomes more reliable.

Proactive machine-learning models in the anti–money laundering domain are being developed to assign a risk rating to each individual or account, indicating the likelihood of fraudulent behaviour.

These models are based on factors such as customer typology, number and type of products held, services used, and transactional behaviour associated with the account.

By way of example, an account with direct debits, a regular salary deposit, and loan repayments is far less likely to be a mule account than a recently created account opened through digital onboarding, classified under a student profile, with no associated products or services, a low average balance, and frequent inbound and outbound transactions.

The importance and effectiveness of these models become particularly evident when they are integrated with transaction monitoring tools, whether focused on incoming flows (AML) or outgoing flows (fraud).

Transaction Monitoring

Transaction monitoring is the key component in the operational chain for detecting money mules. It essentially involves:

- Analysis of alerts generated by monitoring tools.
- Decision-making based on the outcome of that analysis, which may involve measures that create significant customer friction, such as blocking accounts, user access, cards, or other services.
- Verification of legitimacy, whereby additional information and documentation are requested to determine whether the case involves an actual mule or a false positive.
- Termination of the relationship if the case is confirmed, or reversal of the measures taken if the alert proves to be a false positive.

Transaction monitoring tools, whether designed for fraud detection or AML purposes, are based on machine-learning models, yet they operate in a reactive manner. They analyse each transaction in real time, combining it with additional information related to the customer, devices, digital signatures, and other contextual signals at the moment the transaction occurs.

Because this monitoring is conducted in real time, and despite significant technological progress, there are still limitations in the volume and depth of information that can be processed instantaneously. For this reason, integrating the outputs of proactive models into these monitoring systems represents a significant advancement.

The treatment of mule accounts also varies depending on the origin and destination of the funds involved.

1. Victim and mule accounts within the same institution.These are transactions in which both the victim's account and the mule's account are held at the institution being monitored. In this case, detection of the mule is attempted through fraud monitoring tools focused on outgoing transactions from the origin (victim) account. These tools typically assess the "normality" or habitual nature of the transaction initiated by the victim. In such scenarios, integrating proactive models into fraud monitoring systems is particularly important, as enriched rules increase reliability and reduce false positives.

2. Incoming funds from an external bank to a mule account. In this scenario, a mule account within the monitored bank receives funds from another domestic or international institution. Fraud tools are generally designed to analyse outgoing transactions; therefore, since this is an inbound transaction, it must be handled through AML monitoring systems. As in the previous case, integrating proactive models into AML monitoring tools significantly enhances detection effectiveness.

3. Outgoing funds to an external bank. Here, the victim's account is held within the monitored institution, but the funds are transferred to another domestic or foreign bank. Although this is an outgoing transaction, there is no visibility into the destination account, as it belongs to a different institution. This lack of information increases detection complexity and underscores the importance of interbank information sharing and collaborative mechanisms.

Projects are currently being developed to enable the sharing of information on fraudulent accounts across institutions; however, these initiatives are not yet fully operational.

Such mechanisms would significantly facilitate the work currently performed by alert analysts.

Impact of Agent-Based Systems on Operations

Beyond improvements driven by machine-learning models to optimise detection, agent-based systems are expected to become a key component in enhancing operational efficiency.

For example, during the analysis of an alert, specialised agents may conduct preliminary assessments of customer data, transaction data, account information, and associated services or products. An "orchestrator" agent can then consolidate the outputs of these preliminary agents to generate a structured pre-analysis, substantially streamlining and supporting the work that alert analysts currently perform manually.

Carlos Campos Hervas
Head of Financial Crime Operations

What Lies Ahead: Quantum Mules?

Trends by María Angeles Gutiérrez Puente

The money mule phenomenon constitutes one of the operational pillars of contemporary banking fraud. These individuals, whether knowingly or unknowingly, act as intermediaries to move illicit funds and hinder their traceability. However, the emergence of quantum computing and quantum cryptography has the potential to radically transform both the modus operandi of cybercriminals and the defensive capabilities of banks, regulators, and law enforcement agencies.

Quantum Risk: A New Ecosystem for Fraud

The principal threat posed by quantum computing to the financial sector lies in its theoretical ability to break the classical cryptographic schemes upon which banking transactions, digital authentication, and secure communication channels are currently based.

Algorithms such as RSA and ECC could become obsolete once sufficiently powerful quantum computers are developed.

How would this affect money mules? Primarily in two ways:

1. Faster and harder-to-trace fraud.

If an attacker were able to break encryption keys or impersonate digital identities at scale, fraudulent transactions could be generated rapidly, requiring either human or digital mules to move the funds before the attack is detected.

2. The gradual disappearance of the human mule.

Fraud could evolve toward fully automated schemes in which bots and digital wallets, protected by post-quantum cryptographic techniques, manage the movement of funds. The "quantum mule" would take the form of distributed, anonymous software, significantly more difficult to detect and block.

Quantum and Post-Quantum Cryptography: Countermeasures in Favour of Defenders

On the other hand, quantum communications, particularly Quantum Key Distribution (QKD), offer an unprecedented capability: the detection of any interception attempt, based on the quantum no-cloning principle.

If banks adopt QKD between critical centres, interbank communications could become virtually impossible to eavesdrop on, even for an adversary equipped with a quantum computer.

In addition, post-quantum cryptography (PQC), already standardized by NIST, will enable regulators and financial institutions to migrate to quantum-resistant systems before large-scale quantum attacks become a reality.

This implies:

- Reduced likelihood of attacks generating fraudulent transfers, thereby decreasing the volume of illicit funds requiring laundering.
- Improved traceability, as many post-quantum algorithms enable strong authentication without compromising the metadata necessary for investigative purposes.
- Enhanced protection of digital identities and evidentiary material within law enforcement investigations.

Benefits for Criminal Investigation

Quantum computing also holds the potential to strengthen forensic capabilities. For example, it may enable:

- The analysis of large transaction graphs to identify mule patterns with greater depth and speed.
- More efficient correlation of accounts, devices, and behavioural indicators.
- Accelerated blockchain analytics in "crypto-fraud" investigations.

The objective is not merely to improve traceability, but to anticipate behaviour through quantum-enhanced models applied to time series data and financial flows.

Regulators and the Quantum Challenge

Regulatory authorities will need to:

- Mandate migration to post-quantum cryptography.
- Establish clear standards governing the use of Quantum Key Distribution (QKD) in critical infrastructures.
- Develop legal frameworks to address scenarios in which mules take the form of autonomous software rather than human actors.

Maria Angeles Gutiérrez Puente
Head of Cybersecurity & Quantum Financial Crime

Vulnerabilities

Critical Vulnerability in SolarWinds Web Help Desk

Date: 29 January 2026
CVE: CVE-2025-40551

CVSS: 9.8

CRITICAL

Description

A critical vulnerability, identified as CVE-2025-40551, has been discovered affecting SolarWinds Web Help Desk. The flaw is related to an issue involving the deserialization of untrusted data.

Deserialization is the process by which an application converts a stream of data, such as a string or a sequence of bytes, into usable objects within its operating environment.

In this case, the vulnerability could enable remote code execution (RCE), allowing an unauthenticated attacker to execute arbitrary commands on the affected server and thereby compromise the security of the system.

Solution

It is recommended to:

- **Limit Internet exposure** of the affected system and review logs for any indicators of compromise.
- **Upgrade vulnerable servers** running Web Help Desk to version 2026.01 to remediate the issue.

Affected products

SolarWinds Web Help Desk en las versiones 12.8.8 HF1 y todas las anteriores.

References

- thehackernews.com
- incibe.es
- solarwinds.com

TLP:WHITE

Vulnerabilities

Critical Vulnerability in Ivanti EPMM

Date: 30 January 2026
CVE: CVE-2026-1281 and an additional related vulnerability

CVSS: 9.8

CRITICAL

Description

Critical code injection vulnerabilities have been identified in Ivanti Endpoint Manager Mobile (EPMM).

These vulnerabilities (**CVE-2026-1281 and CVE-2026-1340)** allow an attacker to execute remote code without authentication, affecting internal components of EPMM. Ivanti has confirmed that at least one of these vulnerabilities has been actively exploited in a limited number of cases.

Successful exploitation could grant an attacker full control over the EPMM system, compromising mobile device management and potentially enabling unauthorised access to corporate resources.

Solution

It is recommended to:

- Immediately apply the hotfix provided by Ivanti (RPM 12.x.0 or 12.x.1), noting that the hotfix does not persist after a version upgrade and must therefore be re-applied if the system is updated.
- Upgrade to version 12.8.0.0, which will include a permanent fix (scheduled for release in Q1 2026).

Affected Products

Ivanti Endpoint Manager Mobile (EPMM) Affected Versions:

- 12.5.1.0 and earlier
- 12.6.1.0 and earlier
- 12.7.0.0 and earlier

References

- nvd.nist.gov
- hub.ivanti.com

Microsoft Patches Critical Zero-Day Vulnerability in Microsoft Office

Date: 26 January 2026
CVE: CVE-2026-21509

Critical

Description

The vulnerability **CVE-2026-21509** involves a security mechanism bypass in Microsoft Office. It allows an attacker to evade built-in protections through specially crafted documents.

Exploitation requires the victim to open the malicious file, which may lead to the execution of unauthorised actions that compromise the security of the affected system.

Microsoft confirmed that the vulnerability was being actively exploited in the wild. In response, the company released an emergency patch to address the issue immediately.

Affected Products

The products affected by this vulnerability include:

- Microsoft Office 2016
- Microsoft Office 2019
- Office LTSC 2021/2024
- Microsoft 365 Apps

Solution

It is recommended to:

- Immediately apply the security updates released by Microsoft via Windows Update or Microsoft Update.

References

- cyber.gov.rw
- msrc.microsoft.com

TLP:WHITE

Fortinet Patches Critical Authentication Bypass Vulnerability

Date: 28 January 2026
CVE: CVE-2026-24858

Critical

Description

The critical vulnerability **CVE-2026-24858** involves an authentication bypass in FortiOS, the Linux kernel–based operating system used by Fortinet devices.

The flaw could allow an attacker with a FortiCloud account and a registered device to access other devices and accounts without authentication. This capability may have been leveraged to create local administrator accounts, maintain persistence, modify configurations, enable VPN access, and exfiltrate firewall configuration data.

The vulnerability affected several products within the Fortinet ecosystem, including FortiManager and FortiProxy.

Affected Products

The products affected by this vulnerability include:

- FortiManager and FortiAnalyzer services in versions prior to and including 7.6.0.
- FortiProxy versions prior to and including 7.6.4.
- FortiWeb versions from 7.4.0 through 8.0.3.

Solution

It is recommended to:

- **Upgrade to the latest available software versions**
- **Reset any credentials that may have been affected.**

References

- thehackernews.com
- incibe.es

Events

RootedCON 2026
5–7 March

Madrid is preparing to host a new edition of RootedCON 2026, one of the most prominent cybersecurity conferences at both the national and international levels. The event, which will once again bring together technical experts, researchers, security leaders, law enforcement agencies, and technology companies, continues to establish itself as a strategic forum for knowledge exchange and for staying up to date on emerging threats.

Link

Ohio Information Security Conference
11 March

The Ohio Information Security Conference (OISC) 2026 is shaping up to be one of the most important cybersecurity events on the calendar for technical professionals and risk managers. Organised by Technology First, this annual conference will take place on 11 March 2026 at the Sinclair Conference Center in Dayton, Ohio (USA). The event will bring together experts, analysts, CISOs, and security teams to examine the latest threats, real-time response strategies, and innovative solutions to emerging risks particularly those driven by artificial intelligence. The conference will also offer networking opportunities, workshops, and demonstrations of advanced defense technologies.

Link

RSAC Conference
23 - 26 March

The RSAC Conference 2026, widely regarded as one of the most influential events on the global cybersecurity calendar, will once again bring together thousands of industry professionals from 23 to 26 March 2026 at the Moscone Center in San Francisco (USA).The event, where “the world talks security”, serves as a platform to explore the trends shaping the digital future, featuring keynote speeches, technical sessions, and exhibitions on key topics such as artificial intelligence, risk management, identity, and defence against emerging threats. It also provides extensive networking opportunities for researchers, CISOs, and solution providers.Over the years, the conference has established itself as a leading forum for sharing defence strategies, analysing recent incidents, and fostering innovation in cybersecurity.

Link

5th Andalucía Cybersecurity Congress
24 - 25 March

Málaga is preparing to host the 5th Andalusia Cybersecurity Congress on 24 and 25 March 2026, an annual forum that has become a key meeting point for the digital security ecosystem in southern Spain. Organised by the Andalusian Digital Agency in collaboration with Málaga City Council, the event will bring together specialists, institutional leaders, technology companies, start-ups, and SMEs to discuss topics such as data protection, cyber resilience, cloud security, artificial intelligence applied to digital defence, and the growing need for specialised cybersecurity talent.

Link

Resources

- ***Best Practices Checklist***

A current operational cybersecurity action list covering identity controls, critical updates, verified backups, vendor controls, and more. It is ideal as a practical checklist for rapid inspections or internal audits

Link

- **Global Cybersecurity Outlook 2025 – World Economic Forum (WEF)**

A strategic global report examining how cybersecurity is evolving in response to emerging technologies, geopolitical tensions, and resilience challenges. It provides key data on risks such as supply chain dependencies, increasing attack sophistication, and capability disparities among organisations, along with recommendations for leaders navigating this growing complexity.

Link

- **GCA Cybersecurity Toolkit (Global Cyber Alliance)**

A practical toolkit and set of guidance resources designed to help organisations assess their security posture, strengthen common controls, and access free security solutions aligned with internationally recommended baseline defences.

Link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com