CYBERA™

Mule Intelligence Report

H2-2025

TLP Amber Classified

Executive Summary

The second half of 2025 marked a significant evolution in global mule account activity. CYBERA collected more than 16,000 mule accounts across a wide spread of global banks during 2H 2025, revealing a maturing and increasingly diversified threat landscape. While the United States remains the top destination for mule accounts, its share declined sharply, from 58% of all accounts in July to just 31% by December. The decline was not driven by a shift to a single alternative country, but by broad diversification across geographies.

Three themes define this reporting period:

- Geographic Diversification: Mule account activity spread across more countries month over month, growing from 22 countries in July to 72 by December. The UAE emerged as a notable growth region, rising from the 14th most common mule account country in the summer and early fall timeframe to 5th by December.
- Regional Banking Differences: European mule accounts are fundamentally different from the rest of the world. A majority (51%) of European mule accounts are at neobanks/fintechs, while outside Europe major banks dominate at 69%. This reflects criminal adaptation to regional payment infrastructure and consumer banking behavior.
- Account Persistence: More than 1,600 accounts were observed across multiple engagements, and 28% of these had a lifespan exceeding 30-days – suggesting consistent gaps in detection and follow-up across financial institutions globally.

A newly identified threat actor, 'Diligent Planner,' is highlighted in Section 3 for its sophisticated impersonation of US municipal planning departments, targeting homeowners and developers with fraudulent application fees.
These findings reinforce the importance of cross-institutional intelligence sharing and proactive fraud interdiction.

About this Report

This report covers mule account intelligence collected by CYBERA during the second half of 2025 (July through December). Data was gathered through active scam engagement operations conducted by CYBERA. The accounts identified through these engagements, commonly referred to as money mule accounts, represent financial infrastructure actively used or recently deployed by criminal networks.

General Insights

16K+	**Mule accounts collected in H2 2025 across all CYBERA Sources.**
105+	**Countries represented by banks holding identified mule accounts during the reporting period.**
72	**Countries linked to mule accounts in December 2025 alone, up from just 22 countries in July 2025.**

Overall Country Distribution

The United States accounted for the largest share of mule accounts in H2 2025 with 4,750 accounts identified, followed by the United Kingdom (1,591), Canada (546), UAE (472), and Germany (434) to round out the top 5.

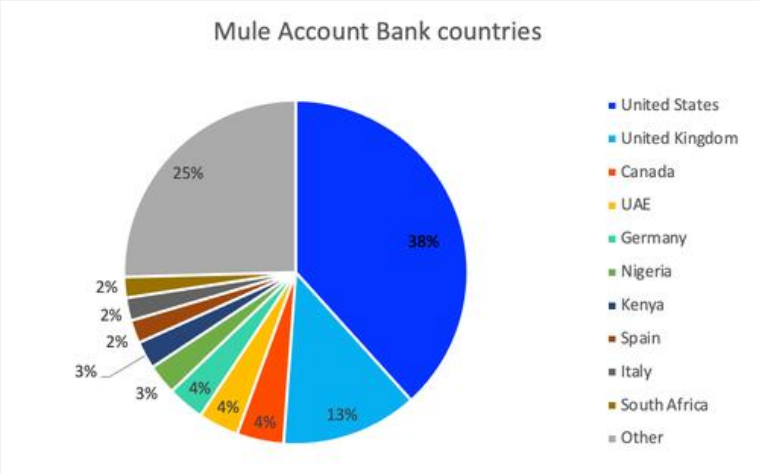

Table 1: Top 10 Countries by Mule Account Count, H2 2025

Growth in Country Diversity

One of the most striking findings of H2 2025 is the rapid expansion in the number of countries linked to mule accounts. In July, accounts were traced to banks in just 22 countries. By December, that number jumped to 72 – a more than 3x increase in geographic spread over six months.

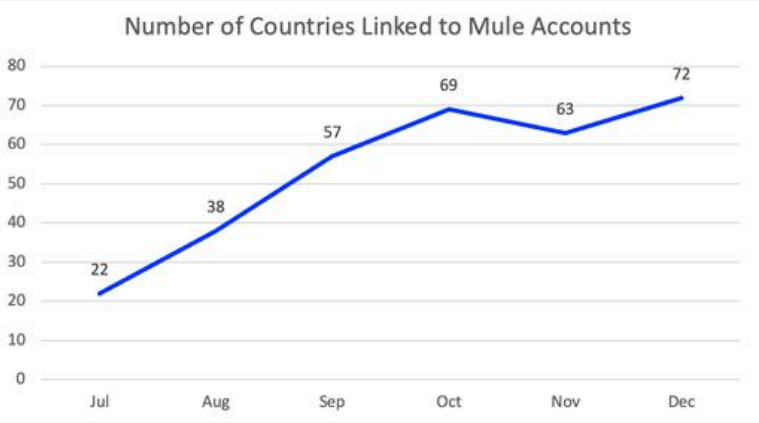

Table 2: Number of Countries with Mule Accounts by Month, Jul-Dec 2025

This jump represents the scaling of CYBERA's AI powered-intelligence system which expanded the data collection footprint substantially.

Mule Account Insights

Declining U.S. Share Amid Broader Diversification

While the United States remains the single largest country for mule account activity, its share of total accounts dropped significantly over the reporting period. In July, 57.5% of all mule accounts identified were U.S. based. By December, that figure had fallen to 30.7%, a decline of nearly 27 percentage points.

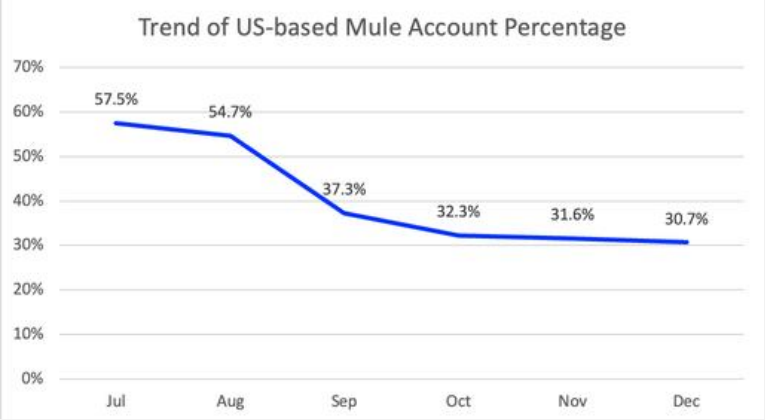

Table 3: US Account Percentage by Month, Jul-Dec 2025

Importantly, this shift does not appear to represent a wholesale migration to another specific country. Rather, the data indicates a broad diversification, with criminals placing accounts across an ever-growing set of countries. The number of countries linked to mule accounts grew during the review period, confirming a geographic spread rather than a concentrated pivot.

Rise of UAE Mule Account Activity

The United Arab Emirates stands out as the most dramatic growth story of H2 2025. Between July and October, the UAE ranked 14th among countries for mule account volume. By November and December, it had risen to 5th place – a significant jump that warrants close attention.

In raw volume terms, UAE-linked accounts grew from just 3 per month in July to 98 in November and 100 in December.

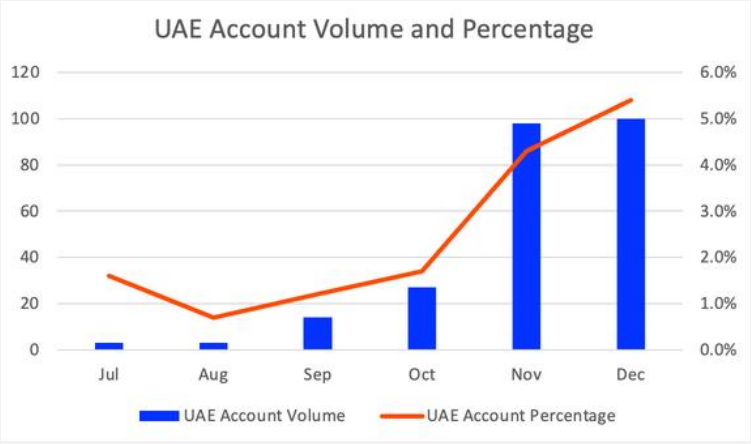

Table 4: UAE Account Volume & Percentage by Month, Jul-Dec 2025

As a percentage of total mule accounts, UAE's share grew from 1.6% in July to 5.4% by December.

Key Insight: The UAE has increasingly become a destination for West African expatriate scammer communities. This population shift may be contributing to the growing use of UAE-based bank accounts in global fraud operations.

Bank Type Distribution: Europe vs. The Rest of the World

One of the most analytically significant findings in H2 2025 is the divergence in bank type preferences between European and non-European mule accounts. This distinction has important implications for financial institutions assessing their exposure.

European Mule Accounts

In Europe, neobanks and fintechs are the dominant vehicle for mule account activity, accounting for 51% of European accounts (1,330 accounts). Major banks represent only 32% of European mule activity (844 accounts), followed by community banks (212), and regional banks (195).

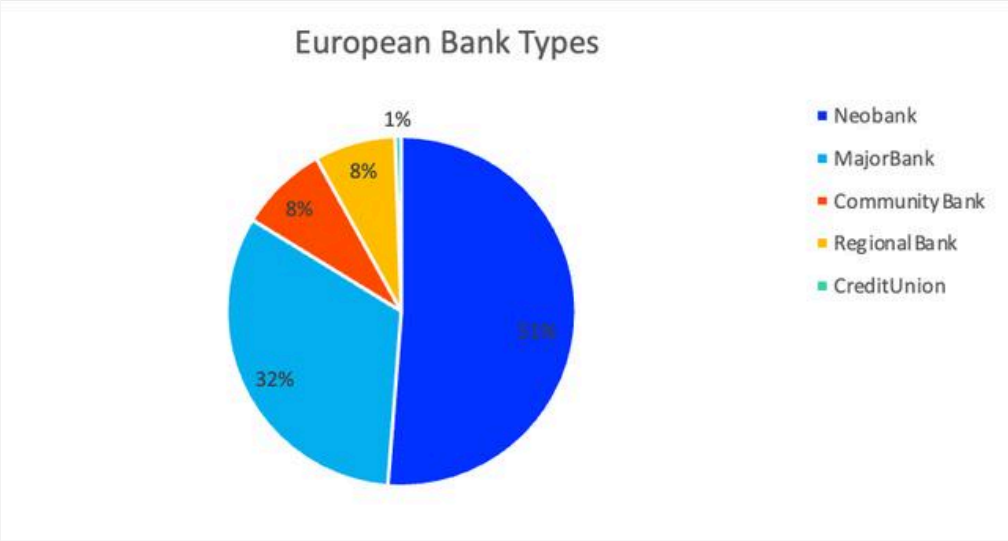

Table 5: European Mule Accounts by Bank Type

Key Insight: France stands out as a notable outlier in the H2 2025 data: approximately 33% of French mule accounts are tied to government impersonation scams. This is meaningfully higher than the global baseline and suggests that scam operators targeting French victims or institutions are disproportionately leveraging government impersonation as a social engineering tactic. This pattern may reflect the credibility that official government communications carry with victims, or the existence of specific threat actors who have developed capabilities targeting French-speaking populations.

Non-European Mule Accounts

Outside Europe, the pattern is nearly inverted. Major banks dominate at 69% of non-European mule accounts (3,346 accounts), while neobanks account for only 8% (356 accounts). Community banks (535), regional banks (355), and credit unions (248) make up the remainder.

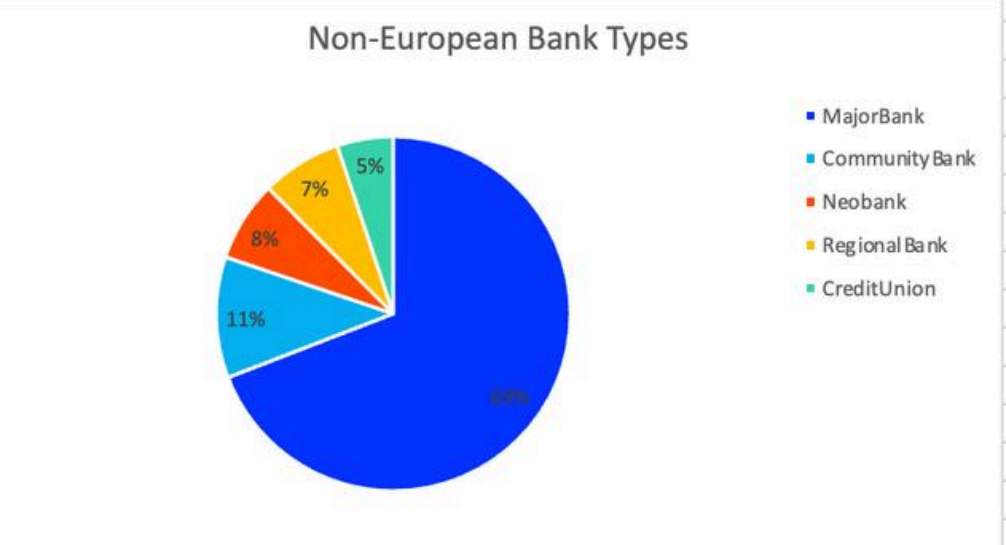

Table 6: Non-European Mule Accounts by Bank Type

Why the difference?

The divergence is best explained by regional banking infrastructure and consumer behavior, not by difference in compliance posture:

- Europe's neobank dominance reflects a mature digital banking ecosystem. Low-friction onboarding, instant payment rails, and high mainstream consumer adoption make neobanks efficient vehicles for fast mule account setup and rapid fund movement.
- Outside Europe, major banks remain dominant because victims are more likely to trust and send funds to accounts at well-known institutions. Criminals place mule accounts where victim payment behavior is most predictable.
- Remote account management is an added benefit. In both regions, criminals prefer institutions where accounts can be opened and operated without in-person interaction.

Account Lifespan: Longer Than Expected

A significant finding in H2 2025 is that mule accounts remain active far longer than might be expected if financial institutions were consistently detecting and closing compromised accounts. More than 1,600 mule accounts were observed across multiple CYBERA engagements – with one account appearing in 25 separate engagements between September and December.

Among accounts seen in multiple engagements, 28% had a lifespan of 30 days or more, meaning the window between when an account was first collected and when it was last collected exceeded one month.

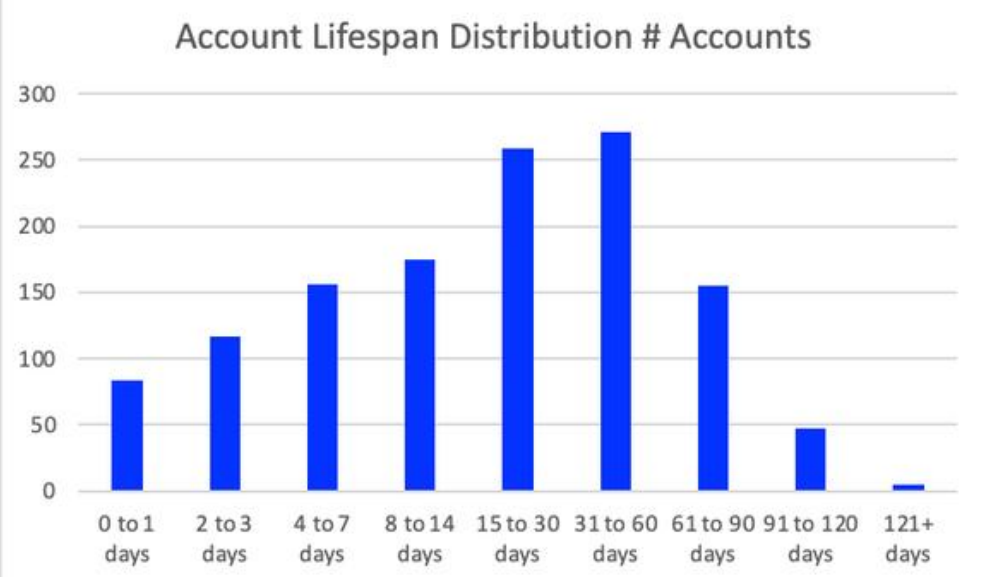

Table 7: Account Lifespan Distribution in Days

Notably, the bank type, bank country, and bank alias distribution for long-lifespan accounts (30+ days) is not materially different from the overall distribution of all mule accounts. The top bank countries for 30_day accounts were the United States, Great Britain, Nigeria, and Canada.

Key Insight: Long account lifespan does not appear to be driven by specific geographies or banking models. Instead, it suggests systemic gaps in detection, internal reporting workflows, or follow-up actions once an account is initially identified as compromised. This points to an industry-wide detection and response challenge rather than a localized one.

Threat Group Highlight

Threat Actor Spotlight: “Diligent Planner”

Beginning in September 2025, CYBERA identified a recurring threat actor – internally designated as “Diligent Planner” - conducting a targeted fraud campaign against homeowners and real estate developers in the United States. As of this reporting period, 21 distinct engagements have been conducted with this actor or their network.

Methodology

Diligent Planner impersonates the planning and zoning departments of local U.S. municipalities. Their targets are individuals and developers who have recently submitted applications to local planning commissions – a highly specific and operationally sophisticated selection of victims.

Scam Communications claim that a fee is required in connection with a recently submitted planning application. The context provided is highly plausible: scammers appear to leverage open-source documents and public records posted on municipal websites to identify active applicants and tailor their outreach with legitimate-sounding details about the specific application.

The Planning Department has completed its formal evaluation of the variance application submitted on behalf of the petitioners and property owners, Sean and Stacey LaPine, for the property located at 1402 Donald Avenue, identified as Parcel No. 25-9103-91280-91001. The request pertains to a non-use (dimensional) variance to permit the construction of a second-story addition to an existing nonconforming single-family dwelling.

The application seeks specific variances associated with the existing nonconforming structure and its yard setbacks. As described in the submitted materials, the requested relief includes:
(a) authorization to alter and expand a legally nonconforming structure;
(b) a waiver of 1.25 feet from the minimum required 8-foot west side yard setback along North Vermont Avenue; and
(c) a waiver of 1.5 feet from the minimum required 30-foot north front yard setback.

The intent of these variances is to facilitate a second-story addition along the front of the existing dwelling while maintaining the structure in its current location on the lot.

Planning staff has conducted a comprehensive review of the proposal, including analysis of the existing nonconforming conditions, the requested dimensional relief, and the relationship of the proposed second-story addition to adjacent properties and the surrounding neighborhood context. Consideration was given to applicable zoning standards, including setback requirements, nonconforming structure provisions, and the criteria for granting dimensional variances. Based on this review, staff has issued a recommendation supporting the application's advancement toward approval by the appropriate decision-making body.

In connection with this recommendation, an Application Approval and Evaluation Fee Invoice has been issued and is attached for your review. Please be advised that **THIS FEE IS ESSENTIAL AND MUST BE SETTLED PROMPTLY TO ALLOW THE APPLICATION TO PROCEED TOWARD FINAL APPROVAL AND INCLUSION ON THE AGENDA FOR FORMAL ACTION.** The fee reflects staff time and resources already dedicated to the evaluation of the variances, as well as the additional work required to complete the process.

The fee directly supports the following components of the planning and zoning review process:

- Application management: Case intake, file establishment, record maintenance, internal routing, and preparation of formal staff documentation and recommendations.
- Site visits and inspection: Field verification of existing conditions, nonconforming elements, and assessment of the proposed second-story addition in context.
- Planning rules and regulation compliance checks: Evaluation against applicable zoning ordinance provisions, dimensional variance criteria, nonconformity regulations, and related municipal standards.
- Contract staff management: Coordination and oversight of any external technical reviewers or consultants engaged to assist in the assessment of the application.
- Overall application management: Preparation of staff reports, agenda materials, draft findings and conditions, and post-decision processing and recordkeeping.

Next steps:

1. Reply to this email to request wire instructions for settlement of the Application Approval and Evaluation Fee Invoice.
2. Settle the invoice in full using the wire instructions once they are provided.
3. Return the wire receipt so that payment may be confirmed and the application scheduled for agenda placement and formal consideration.

Your prompt attention to this matter will ensure that the application continues forward smoothly and receives full consideration at the Commission level. Should you have any questions regarding the invoice, payment procedures, or any aspect of the application process, please contact this office directly.

Best regards,

Joseph M. Murphy
Director of Planning

Planning and Zoning Commission
City of Royal Oak
203 South Troy Street
Royal Oak, MI 48067

Scammer Communication - Diligent Planner

About CYBERA™

CYBERA was founded by former cybercrime prosecutors to disrupt the scam economy by targeting the infrastructure that makes scams possible: **money mule accounts.**

CYBERA deploys an AI-powered, agentic scam engagement system that interacts directly with scammers at scale to extract confirmed, evidence-backed mule accounts before funds are transferred and lost.

These accounts - used by criminals to receive and launder stolen funds - are identified directly from scammer communications, not inferred through probabilistic modeling.

CYBERA shares high-fidelity mule intelligence with financial institutions to:

- Detect and action on-bank mule accounts to reduce money laundering exposure.
- Screen outbound payments against known off-bank mule accounts to stop scam losses before funds move.
- Strengthen fraud, AML, and cyber investigations with contextual, defensible intelligence.

Unlike behavioral risk scores, CYBERA's mule intelligence provides a clear, pre-loss signal tied to known scam activity - enabling confident operational and regulatory action.

For more information please visit www.cybera.io.