CYBERA™ Scam Intelligence Report

Q3-2025

FS-ISAC

TLP Amber Classified

Executive Summary

Q3 2025 marked a notable escalation in global scam activity, with 3,696 mule accounts identified across 743 banks in 122 countries. The data reveals a broadening operational footprint and increasing coordination among scam networks.

Major banks accounted for nearly 60% of identified mule accounts, continuing a pattern of concentrated risk within large institutions, while Fintech/Neobank exposure grew to 22%, reflecting criminals' shift toward faster-moving digital platforms.

Geographically, the United States and United Kingdom continued to dominate global mule activity, while Canada, UAE, and Nigeria emerged as notable growth regions. Canada in particular saw a steady rise in account detections through the quarter, suggesting a widening operational footprint of scam networks within North America.

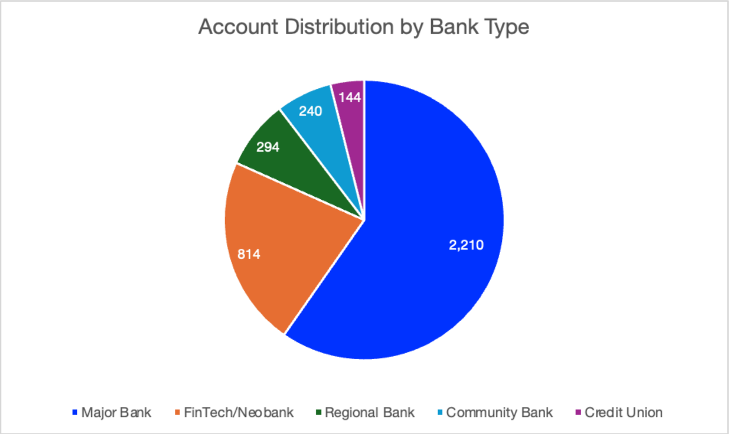
A new global threat actor, "Dr. Placebo," was also identified during the quarter. This actor operates under the guise of pharmaceutical legitimacy to build trust with victims and has been linked to 58 unique mule accounts across multiple continents. The emergence of such coordinated campaigns underscores the increasing sophistication and adaptability of global mule herders.

These findings highlight the value of the FS-ISAC Fraud Feed in enabling early interdiction and intelligence sharing across the financial ecosystem—helping member institutions move decisively left of boom to prevent loss before funds move.

General Insights

Distribution of Accounts by Bank Type

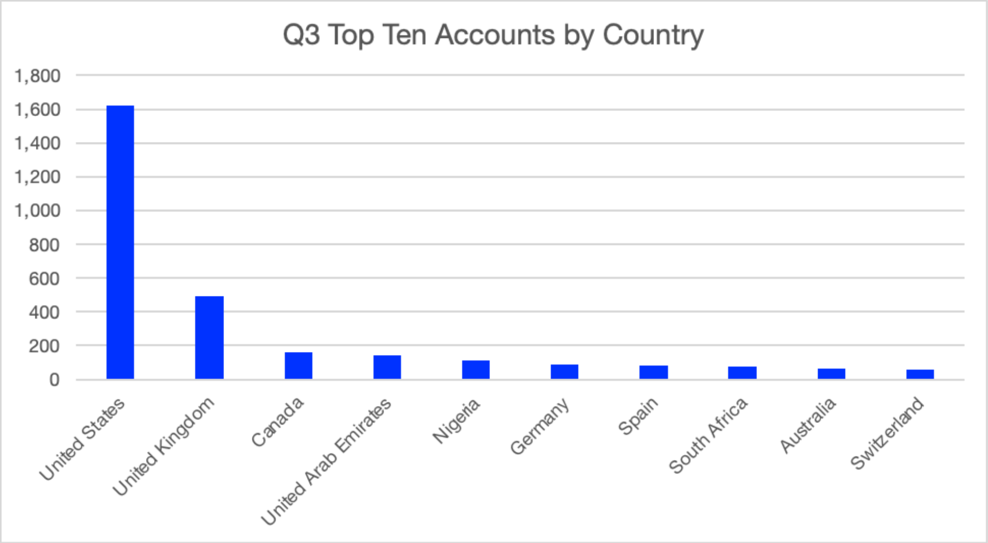
Major Banks accounted for the majority of mule accounts (59.7%), continuing a trend of concentration within large, consumer-facing institutions. FinTech and Neobank activity rose to 22% (814 accounts), reflecting criminals' growing use of fast-onboarding digital platforms. The remaining 18% (678 accounts) were spread across Regional Banks (294), Credit Unions (144), and Community Banks (240). This diversification indicates that no single segment is immune to exploitation, and that mule recruitment continues to adapt to available banking channels.



Q3 Distribution of unique accounts by bank type

Distribution of Accounts by Country

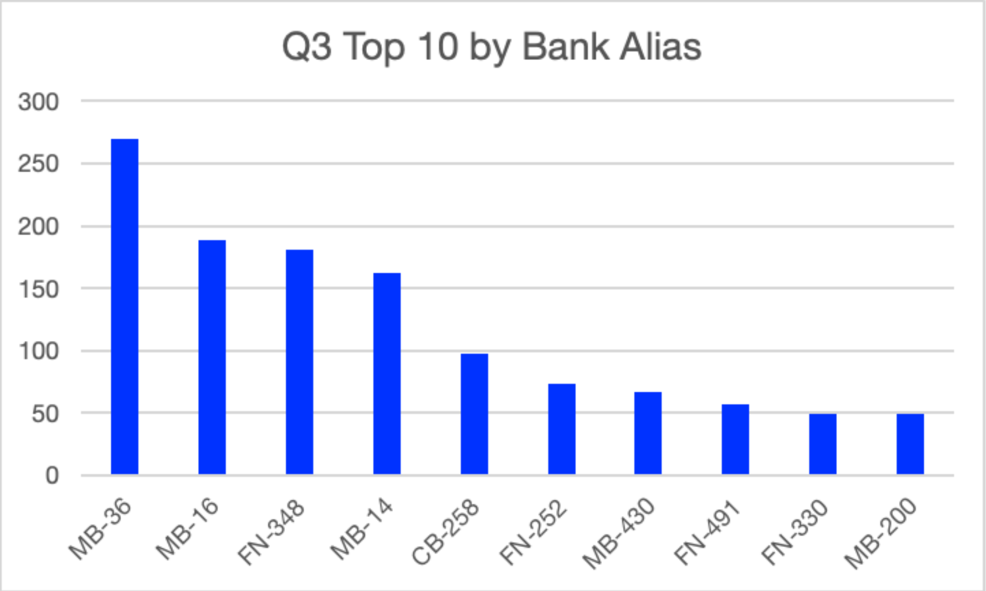
In Q3 2025, the United States accounted for the largest share of mule accounts by far, with over 1,600 accounts. The United Kingdom followed with around 490 accounts. Other countries in the top 10 included Canada, United Arab Emirates, Nigeria, Germany, Spain, South Africa, Australia, and Switzerland. This wide geographic spread highlights the truly global footprint of scam networks and underscores the need for collaborative international countermeasures.



Distribution of accounts by country

Distribution of Accounts by Bank Alias

As anticipated, the Top 10 mule account list by anonymized bank alias is largely dominated by Major Banks. While they account for 62% of total mule activity and FinTech/Neobanks represent 30%, the appearance of a Community Bank making up just 8% overall is a notable outlier and highlights that no segment is immune.

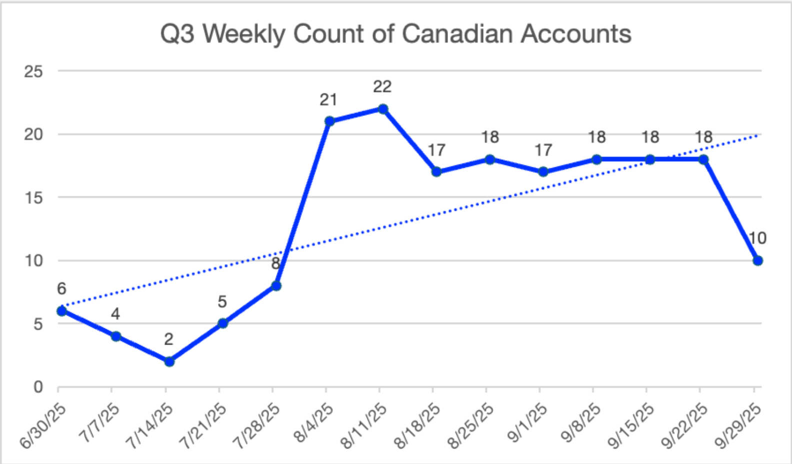


Anonymized Top 10. MB: Major Bank, FN: FinTech/Neobank, RB: Regional Bank, CU: Credit Union, CB: Community Bank

Spotlight on Canada

Rise in Canadian Accounts

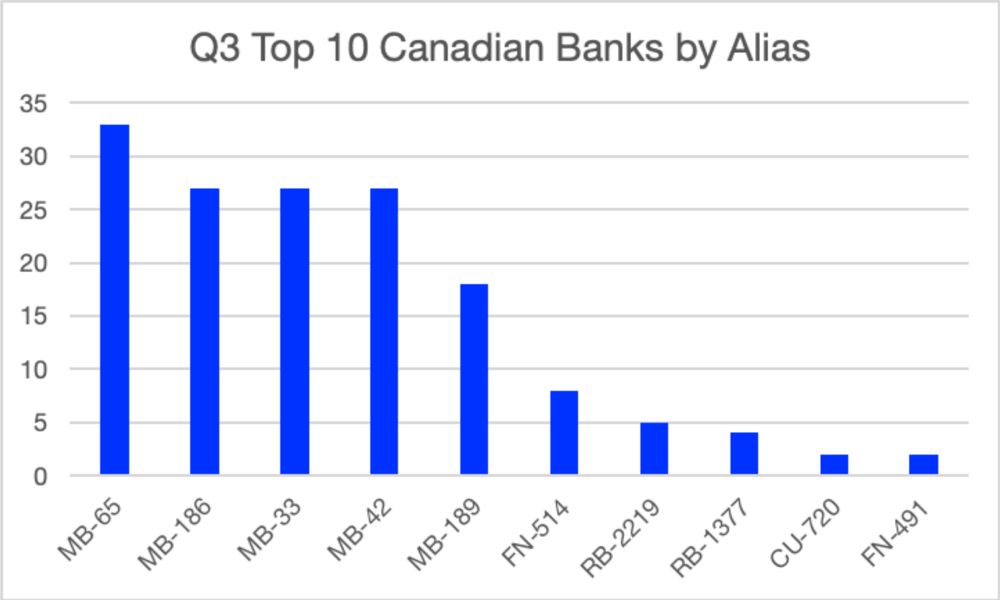
Canada experienced a steady rise in mule account activity throughout Q3, reflecting growing scam and fraud operations targeting domestic financial institutions. Activity increased from just 4–8 distinct accounts per week in early July to a peak of 22 accounts by mid-August, maintaining elevated levels through September before tapering at quarter's end.



Weekly count of unique bank account ID

Distribution of Accounts by Bank Type

The concentration of activity was heavily skewed toward major banks, which accounted for most of the identified accounts—led by MB-65 (33), MB-186 (27), MB-33 (27), and MB-42 (27)—with smaller volumes observed among fintech/neobank and regional bank categories. The persistence of activity across multiple major banks suggests coordinated mule usage patterns rather than isolated events, underscoring the need for continued monitoring and cross-institutional intelligence sharing within the Canadian ecosystem.



Anonymized Top 10. MB: Major Bank, FN: FinTech/Neobank, RB: Regional Bank, CU: Credit Union, CB: Community Bank

Mule Ring Insights

CYBERA's 2025 Mule Ring Report, will be released at FS-ISAC's Spring Summit in March 2026, the report covers characteristics and analytics of mule rings including:

1. **Bank Type Affinity:** Measure Mules Ring affinity for specific Bank Types (e.g. Major Bank or FinTech) as measured by a disproportionate portion of accounts at that bank type.
2. **Geographical Affinity:** Measure Mule Ring affinity for specific geographical locations.
3. **Bank Affinity:** Measure Mule Ring affinity for specific banks (anonymized).
4. **Account Promiscuity:** Measure each Mule Rings distribution of their money mule accounts.

To request a copy of CYBERA's earlier report on Mule Rings, contact us at fsisac@cybera.io.

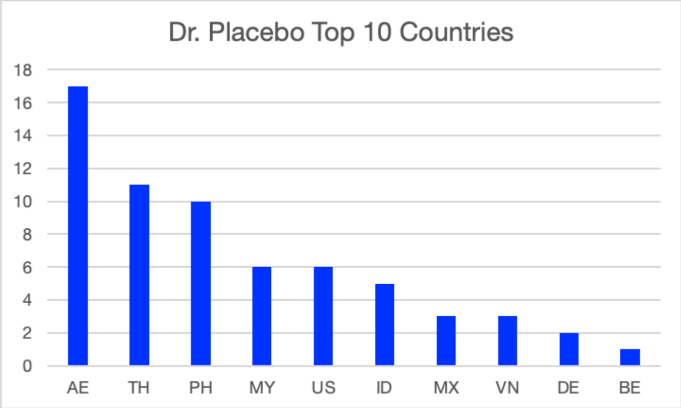
New Mule Ring #1: "Dr. Placebo"

Q3 reinforced a shift from isolated mule activity to structured, multi-bank mule rings capable of moving funds across regions. This evolution—combined with the rise of specialized herders such as "Dr. Placebo"—signals that organized scam operations are becoming more resilient, data-driven, and internationally connected.

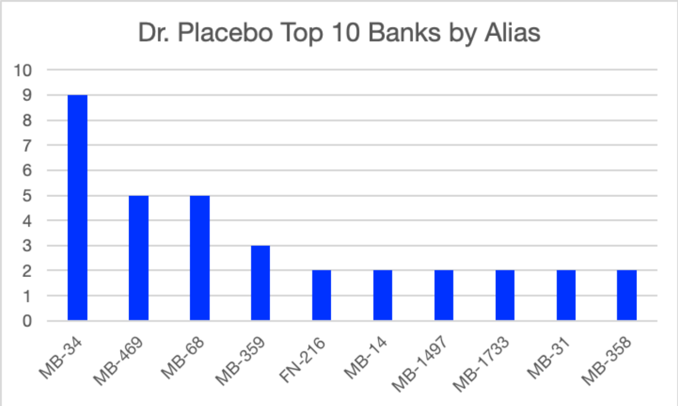
In August, our scam engagement team conducted a outreach campaign, focused on a specific region. Through this effort a new player emerged in our top mule herder category. "Dr. Placebo" entered the scene and has steadily remained at the top of the list. This mule herder disguises activity under the front of pharmaceutical legitimacy to build trust with their victims.

They requested payments to 58 unique accounts, primarily across the UAE and Southeast Asia, but with smaller numbers in other continents inclduing North America. Overall, this threat actor operated accounts in 13 countries indicated a wide network of operations.

Dr Placebo's top 10, in terms of number of accounts by bank, depicted below with anonymized bank aliases, shows mostly Major Banks, with only 1 non-Major Bank present: FinTech/Neobank FN-216.



Top 10 Countries with Dr. Placebo Accounts



Anonymized Top 10 banks impacted by Dr Placebo by number of accounts

About CYBERA™

CYBERA was founded by cybercrime prosecutors to disrupt the scam economy by:

- Obtaining data on scammer financial accounts controlled by criminals and sharing with financial institutions to:
    - Reduce money laundering at their institution
    - Stop scams by preventing fraudulent payments from their institution

CYBERA engages with scammers to extract bank accounts they use to receive and launder funds from scam victims. These transactions are often performed via wire transfers through accounts colloquially known as money mule accounts.

FS-ISAC has collaborated with CYBERA to receive a daily feed of mule accounts and distribute this data feed to FS-ISAC members via SHARE. FS-ISAC will generate alerts in SHARE, empowering organizations to proactively address risks and bolster their cybersecurity and fraud defenses.

For more information on CYBERA, this report or using the FS-ISAC SHARE feed please contact CYBERA at fsisac@cybera.io and www.cybera.io.