LexisNexis®
RISK SOLUTIONS

CASE STUDY

Large Financial Institution Sees 50% Uplift in Detection of Money Mule Accounts During First Year Using LexisNexis® Risk Solutions

LexisNexis Risk Solutions helps bank return $965,000 to victims of money mules

AT A GLANCE

COMPANY

Large Financial Institution

REQUIREMENTS

- Accurately identify and block money mule accounts.
- Block fraudulent funds from being moved by mules.
- Minimize fraud losses associated with money mules.
- Prioritize a frictionless and successful user experience for good customers.

SOLUTION

Using LexisNexis Risk Solutions digital identity intelligence, this large financial institution can accurately identify and block money mule accounts, as well as detect wider mule networks, while prioritizing a frictionless experience for legitimate customers.

BOTTOM LINE

- 50% uplift in volume of money mules identified.
- $965,000 of funds received into mule accounts stopped and returned to victims.
- Minimized friction for good, returning customers.

CASE STUDY

Overview

This large financial institution offers a wide range of services including personal and business banking, private banking, insurance and corporate finance. The customer sits at the heart of the bank's ethos: trust plays an integral part of the institution's aim to be respected and valued by its customers.

Business Problem

Money mules have become a key enabler for a lot of 3rd party fraud and other scams which impact customers and banks across the industry. Cybercriminals, motivated by large financial gain and armed with credentials stolen from numerous data breaches, are becoming adept at taking over genuine online banking accounts. However, once the fraudster infiltrates an account using stolen credentials, or deploys social engineering tactics against a genuine customer, the money must be moved to an account which the fraudster has control over and in which the ill-gotten gains can be laundered.

Defined as someone whose bank account is used to launder the proceeds of crime through the financial system, mules are engaged or recruited, either knowingly or unknowingly, for the purposes of laundering money. Hard to track, money is moved rapidly through large networks of seemingly unconnected mule accounts held at multiple financial institutions.

This large financial institution was faced with the challenge of how to identify money mule activity within their online banking environment, requiring a solution which would not only detect such activity, but also help stop funds from being moved and ultimately returned to the victims of the crime.

"We can now take the fight to the mules, with LexisNexis® Risk Solutions enabling us to adopt a proactive approach to money mule detection. Without that change in approach, we wouldn't be able to return such a substantial sum of money to the victims of these scams."

Establishing Trusted Behavior with LexID® Digital

Since LexisNexis® Risk Solutions was first implemented, the bank has been able to identify 50% more mule accounts and has returned $965,000 of fraudulent funds to the victims of the money mules. Driving this success is the LexisNexis® Digital Identity Network® , which was able to reveal anomalous behavior indicative of money mules by analyzing attributes such as location, device and behavior anomalies.

Leveraging global digital identity intelligence, the bank was able to clearly see the spiderweb of linked accounts generated by mule activity. It could therefore connect known mule devices with new accounts at login, with email alerts, enabling it to quickly block these new mule accounts. Device and IP intelligence was leveraged to link devices and identify additional mules and networks, with the bank, in one instance, uncovering a fraud ring involving 140 mule accounts. The bank was also able to aid in the arrest of a fraudster recruiting mules, with intelligence from LexisNexis Risk Solutions able to pinpoint the location of the mule account activity.

The bank also deployed a mule model that targets unknown mules based on behavior patterns. This allowed it to analyze behavior and patterns at a granular level, and more accurately differentiate between new mules and legitimate behavior change. Allowing for changes in trusted user behavior, the mule model also helped to reduce friction for legitimate customers.

The LexisNexis Digital Identity Network uses anonymized global shared intelligence to better distinguish between customers and fraudsters, underpinned by crowdsourced intelligence from millions of daily consumer interactions including logins, payments, and new account applications across thousands of global businesses.

Key Features of the LexisNexis Risk Solutions / Bank Partnership

- **Trust Tags** are digital labels that enable businesses to define, categorize, tag and differentiate between good and bad users, devices, locations or personas. Trust can be associated dynamically with any combination of online attributes such as devices, email addresses, card numbers or any other attributes involved in accepting, rejecting or reviewing a transaction.

CASE STUDY

- **Smart ID** identifies returning users that wipe cookies, use private browsing, and change other parameters to bypass traditional device fingerprinting tools. Smart ID improves returning user detection and reduces false positives. Derived from the analysis of many browsers, plug-in, and TCP/IP connection attributes, Smart ID generates a confidence score that detects multiple fraudulent account registrations from the same device.
- **True IP** accurately detects the use of location and identity cloaking services, such as hidden proxies and VPNs, allowing the bank to see the true IP address, geolocation and other attributes of each transaction. It can also detect changes in behavior patterns, such as unusual transaction volumes, changes to velocity or frequency of transactions. This dynamic data helps identify fraudulent behavior, providing the bank with a more accurate context of whether any transaction should be accepted, rejected or reviewed.
- **Deep connection analysis technologies** give a clearer view of suspicious events. Fraudsters attempting to open a new account from an unusual or high-risk location may attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and the TOR browser. With Proxy piercing technology, LexisNexis® Risk Solutions examines TCP / IP packet header information to expose both the Proxy IP address and True IP address.

LexisNexis® RISK SOLUTIONS

For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN