RemitSo

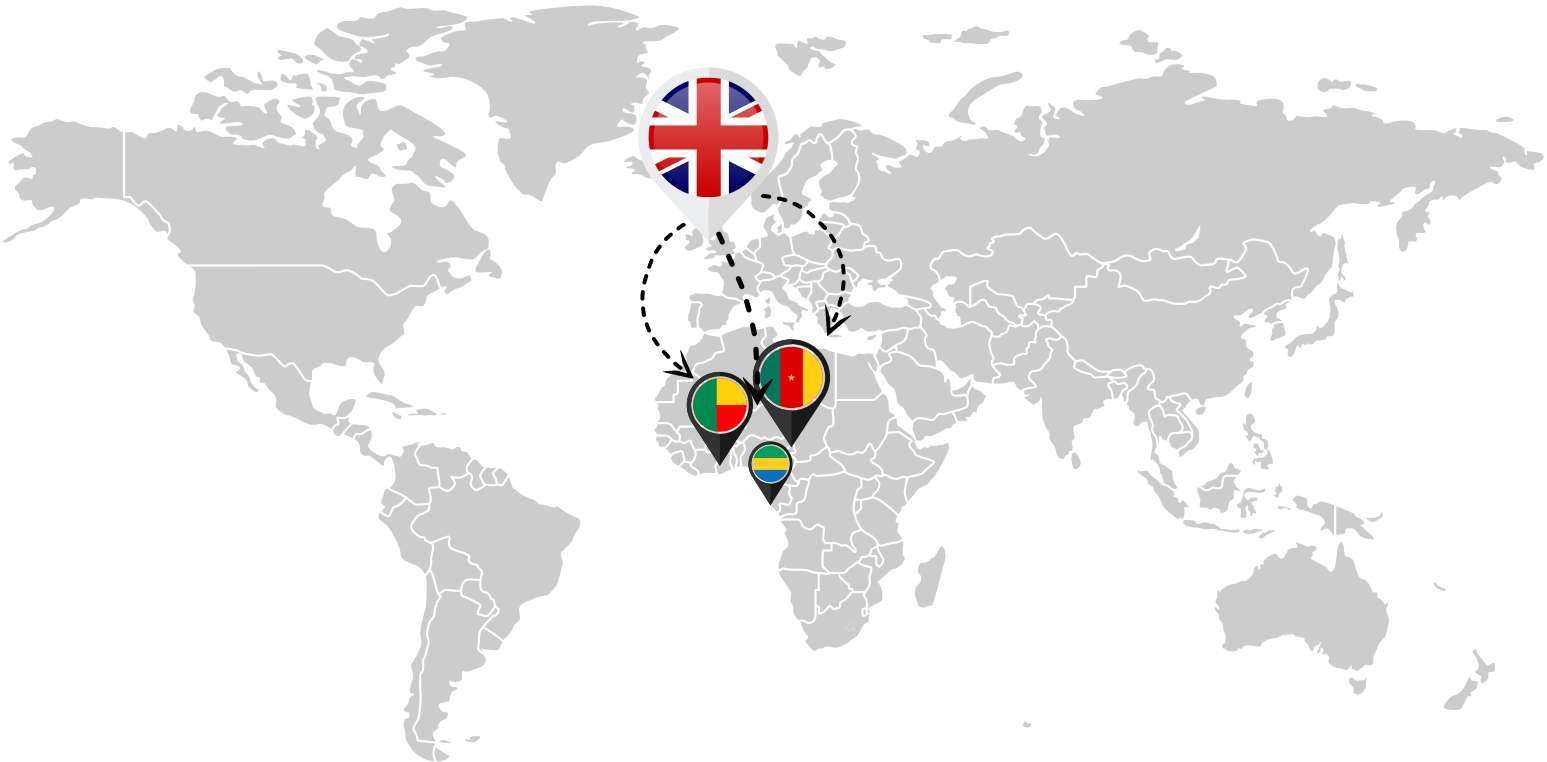
CASE STUDY

Cracking an International Money Laundering Network

The Hidden Trail – From the UK to Nigeria via Benin, Cameroon & Gabon

The Suspicious Transactions Begin

It all started with a pattern that seemed harmless at first—***multiple senders from the UK transferring money to Benin, Cameroon, and Gabon.***
Individually, these transactions looked normal. The amounts were moderate, and the declared purpose was ***business-related transfers.***
But as we examined the flows, ***something wasn't adding up.***
All the money sent to these countries was being ***immediately forwarded to the same bank account in Nigeria.***
This wasn't just a coincidence. It was a ***deliberate, structured money laundering operation.***



Key Red Flags That Raised Suspicions

- **Hundreds of small transactions**, all leading to a single Nigerian bank account.
- **Different currencies (GBP, XAF, XOF) were used,** but after conversion, the GBP amount **always matched** the NGN (Nigerian Naira) total.
- **The recipient was a 29-year-old woman in Nigeria,** yet she had no **business registration or financial background** to justify these inflows.
- **All transfers were labeled as 'business transactions',** yet the invoices provided were either **fake or non-existent.**
- **Same device models and geolocations** were used for multiple UK senders, even though they were supposedly different individuals.
- **Suspicious email addresses—**completely random and unconnected to the sender's identity.
- **The transactions were too precise, too structured—hallmarks of a laundering operation.**

How We Cracked the Case Using Technology & Compliance Measures

At this point, suspicions weren't enough—we needed solid **proof** before taking action.

IP Tracking & VPN Detection

We analyzed the **IP addresses** used by the senders and immediately found:

VPN Usage & IP Masking

- Many senders claimed to be in the UK, but their IP traces led back to West Africa, Eastern Europe, and the Middle East.
- They used datacenter-based VPNs, which fraudsters often use to bypass security checks.

Conclusion: These transactions were not originating from the UK. The senders were masking their real locations.

Device Fingerprinting & Login Analysis

Using **device intelligence tools**, we identified:

Same Device, Different Senders?

- Many transactions were **initiated from the same phone model**, **same operating system, and same browser configurations.**
- Despite being from "different" people, they **originated from the same physical devices.**

Conclusion: A **fraud ring** or **automated laundering script** was at play.

Email Address Analysis

We examined the **email IDs** used for registration and found:

Completely Random Emails

- Many accounts used emails like ***wsfjbsdfgsdbkj@gmail.com*** or ***af43jfdsfkl@yahoo.com.***

Disposable & Fake Identities

- The email names had no connection to the sender names on file.

Conclusion: These weren't **real users**—they were fake identities.

Taking Action: How We Stopped the Laundering Network

Blocking Suspicious Transactions

Once we confirmed our findings, we **blocked all transactions** leading to the Nigerian account.

- **Funds were frozen** to prevent further movement.
- **Senders were flagged** for enhanced due diligence (EDD).

Business Verification & Fake Invoice Detection

We demanded **official invoices and receipts** to justify the transactions.

What we found:

- The invoices were **identical across multiple senders**, suggesting they were fabricated.
- Some businesses **did not exist**, while others had **no financial activity matching the payments.**

Conclusion: The **"business transactions" were fake**—just a cover for laundering.

Enhanced Identity Verification

We took things a step further by requesting **live video verification** from the Nigerian recipient.

- They submitted a **pre-recorded 30-second video**—but the person **did not match the ID card on file.**
- We insisted on a **real-time live video call** with the recipient holding their ID.

That's when they vanished.
No more responses. No more transactions. **The network collapsed overnight.**
They knew **they had been caught.**

Regulatory Implications & Compliance Actions Taken

After confirming this was a **structured money laundering scheme**, we **escalated the case to financial authorities** and took the following compliance steps:

SAR (Suspicious Activity Report) Filing

We submitted **detailed SARs** to financial regulators in:

✅ **The UK** – Financial Conduct Authority (FCA) & National Crime Agency (NCA).
✅ **Nigeria** – Economic and Financial Crimes Commission (EFCC).
✅ **Benin, Cameroon, and Gabon** – Respective financial crime agencies.

This helped **alert law enforcement** about the laundering network.

Strengthening AML (Anti-Money Laundering) Policies

After this case, we **enhanced our fraud detection systems** by:

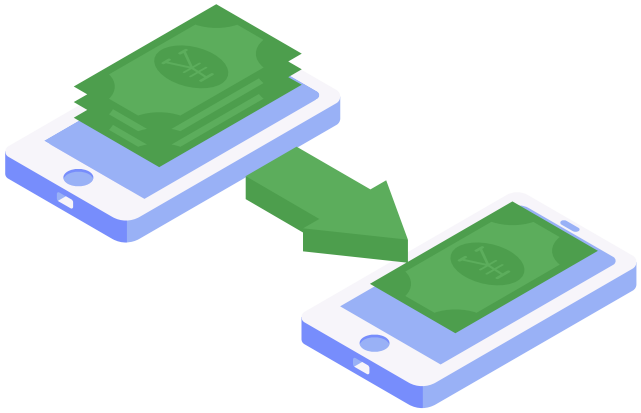
✅ **Implementing stricter IP & VPN monitoring** – Flagging users attempting to transact via masked IPs.
✅ **Enhancing device tracking** – Identifying when multiple accounts use the same device.
✅ **Requiring biometric & live verification for high-risk recipients.**
✅ **Increasing invoice validation** – Using AI to detect duplicate or fake documents.

Cooperation with Banks & Payment Processors

To **prevent similar schemes**, we partnered with:

✅ **Banks in Nigeria & the UK** to cross-check flagged accounts.
✅ **Payment processors** to identify laundering patterns in real-time.

This collaboration helped **shut down fraudulent accounts and prevent future abuse.**



Lessons Learned: How We Stay Ahead of Fraudsters

This case **exposed the advanced tactics used in money laundering** but also proved that **with the right security measures, they can be stopped.**

IP & VPN Detection
Identifying masked locations to expose fraud rings.

Device Fingerprinting
Linking multiple accounts to the same devices.

AI-Based Pattern Recognition
Detecting structured money flows.

Live Video Verification
Fraudsters couldn't fake real-time ID proof.

Regulatory Reporting
Filing SARs ensured legal action.

Fraudsters evolve—but so do we. With the right safeguards, they won't succeed.