Bottomline

Anatomy of a Digital Banking Fraud Attack

How modern fraudsters target digital banking platforms; and how you can stop them

1 Identify & Harvest Credentials

How the Attack Starts:

Long before transactions occur, fraudsters start gathering data and laying the groundwork for their fraud attack.

Their Tactics:

- Phishing & Spoofed Domains
- Scraped Employee Profiles
- Credential Stuffing

Your Superpower:

Detect threats and monitor identities to block attackers **before** they log in.

2 Gain Unauthorized Access

The Breach Begins:

Using stolen credentials, the fraudster impersonates your users, your employees, or your vendors to sneak past security and enter your systems unnoticed.

Their Tactics:

- Phishing & SIM Swapping
- Compromised API Keys
- SSO Misuse

"3rd Party payment fraud is a **growing threat** to commercial customers – All banks surveyed reported rising attack volumes, in particular impersonation frauds and BEC."

- PWC Commercial Banking Fraud Survey, 2025

Your Superpower:

Intelligently authenticate and perform device recognition to stop imposters in their tracks.

3 Escalate Access & Move Laterally

The Power Grab:

Now that the bad actor is "in", they begin to reset passwords, hijack sessions, or exploit third-party systems.

Your Superpower:

Stop internal misuse or malicious external threats with role-based account access and anomaly detection.

4 Execute Fraudulent Transactions

The Money Moves:

Fraudsters strike, initiating real payments through legitimate payment rails, each with unique vulnerabilities.

Payment Rail	Fraud Tactic
ACH	Fake batches, template tampering
Wire	Impersonations, urgent transfers scams
RTP/Zelle	Real-time push scams, spoofed alerts
Card/Wallets	Token fraud, embedded merchant abuse

"**94%** of global fraud executives saw an increase in real-time payments, while 80% reported a rise in mule-account activity on those rails. **APP fraud concerns topped the list at 82%.**"

– Datos Insights / Outseer, 2024

Your Superpower:

Flag and stop suspect payments with real-time risk scoring and embedded fraud logic.

5 Launder Funds & Cover Tracks

Quick Exit:

The attack ends and the fraudsters funnel funds through a web of mules or crypto, and evidence is erased often in minutes.

Visualize a rapid bot executing dozens of transactions, deleting traces, and vanishing—all in under 10 minutes.

Your Superpower:

Keep digital attackers from making a clean getaway with real-time detection and traceability tools.

Stop Fraud in Its Tracks!

Your Defense Arsenal:

Fraud is fast, but your defenses are faster. Equip your digital banking platform with intelligent tools that work around the clock to detect, deflect, and defeat the threats before they strike. These built-in defenses help safeguard your platform. your customers, your reputation and your revenue.

Get Superhero-Grade Controls

- Adaptive MFA & Device Recognition
- AI-Driven Fraud Detection
- Secure APIs
- Payment-Level Risk Scoring
- Internal Threat Management
- Case Management Dashboards
- Ongoing Staff/User Training

Ready to Stop Fraud Attacks Before They Start?

Fraudsters don't wait. Neither should you. Arm your digital banking platform with built-in security and smarter payment protection tools to safeguard against fraud in real time.

Get in Touch

Bottomline

REV US082125LM