EARLY DETECTION OF ADVANCED PERSISTENT THREATS IN THE PAYMENTS SECTOR

The role of real-time transaction monitoring in combatting today's most sophisticated fraud attacks

STANCHION

STANCHION'S EARLY DETECTION FRAUD SOLUTION IN ACTION

Following a major data security breach, one of the largest financial services groups in Africa asked Stanchion for help in architecting and implementing a first line of defence against fraud at ATMs.

It took us just six weeks to roll out a solution that protects the group through early detection of irregular transactions that evade industry standard transaction authentication and fraud detection methods.

THE CHALLENGE

Our client runs a complex payments environment processing millions of transactions every month originating from point of sale devices, ATMs and other transaction points around the world.

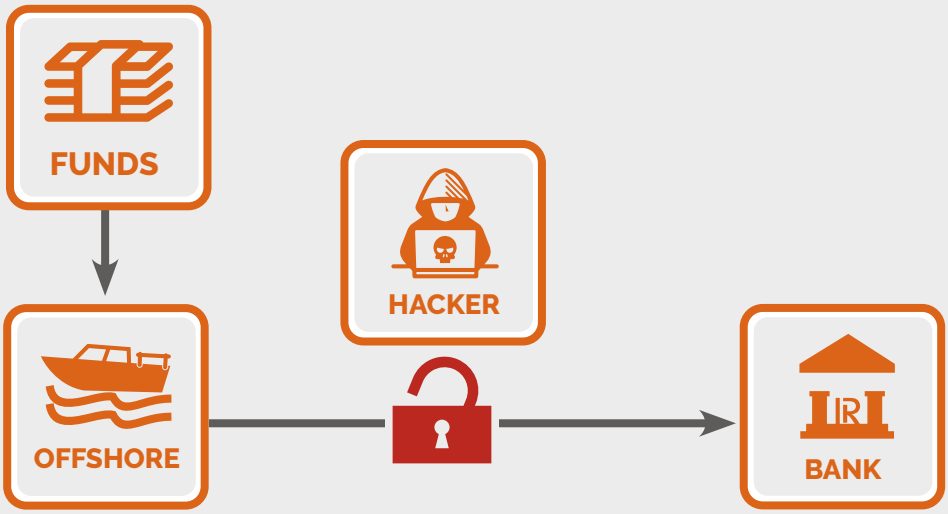
Facing increasingly sophisticated fraud techniques and information security risks – such as targeted man-in-the-middle attacks – the group wanted to implement a reliable, early-warning system to alert it to fraudulent transactions.

Each transaction the group processes must pass through multiple hops from the consumer-facing payments terminal to third-party payments services to the institution's back-end systems. Our solution needed to preserve the performance of our Client's payment systems and so maintain their high-level customer experience. At the same time, the transaction monitoring system needed to be responsive and rigorous enough to stop coordinated global attacks from highly sophisticated crime syndicates.

System Vulnerabilities

Man-in-the-middle (Hacker) attacks can be designed to target the front-end of your payments system.

This makes detecting attacks very difficult for the risk monitoring software that resides on the back-end of your payments system.



THE SOLUTION

Given the complexities of our client's payments environment, an innovative and robust solution was required. They turned to Stanchion for help, based on our experience and expertise within the global payments industry, the financial group's internal environment, and an intimate knowledge of how the payments system works in our client's home territory.

We proposed a sophisticated solution that combined our proprietary skills and services with the INETCO Insight independent transaction monitoring software and data streaming platform. We supported the financial services group by providing consulting, integration, implementation and support services for the rollout.

The solution interfaces with a range of complex payments systems including:

- MasterCard
- Visa
- The national clearing house and payments system operator in our client's home territory
- The Postilion payments engine

Our solution allows the client to trace a transaction from end-to-end, without the use of heavy agents, extra traffic loads or code changes. Easy access to this rich transactional intelligence helps the group quickly isolate potentially fraudulent transactions and prevent processing.

SOLUTION BUILDING BLOCKS

- Stanchion consulting and integration skills
- Stanchion proprietary intellectual property
- Stanchion's trusted relationship with our clients highly sensitive payments ecosystem
- INETCO Insight real-time transaction monitoring software

THE OUTCOME

The financial services group now have an accurate and reliable solution for early detection of fraudulent transactions, protecting it from a range of sophisticated risks without impairing the performance of its payments infrastructure. The platform enables our client to:

- Receive alerts when excessive transaction activity occurs, for example, suspiciously high-velocity transaction volumes at a given ATM and multiple ATM's.
- Identify patterns that indicate fraud, such as when a card is being used at multiple locations at the same time or when a card is used for many high-value transactions, in a short amount of time.
- Receive real-time alerts when unusually large transaction values or volumes are occurring.

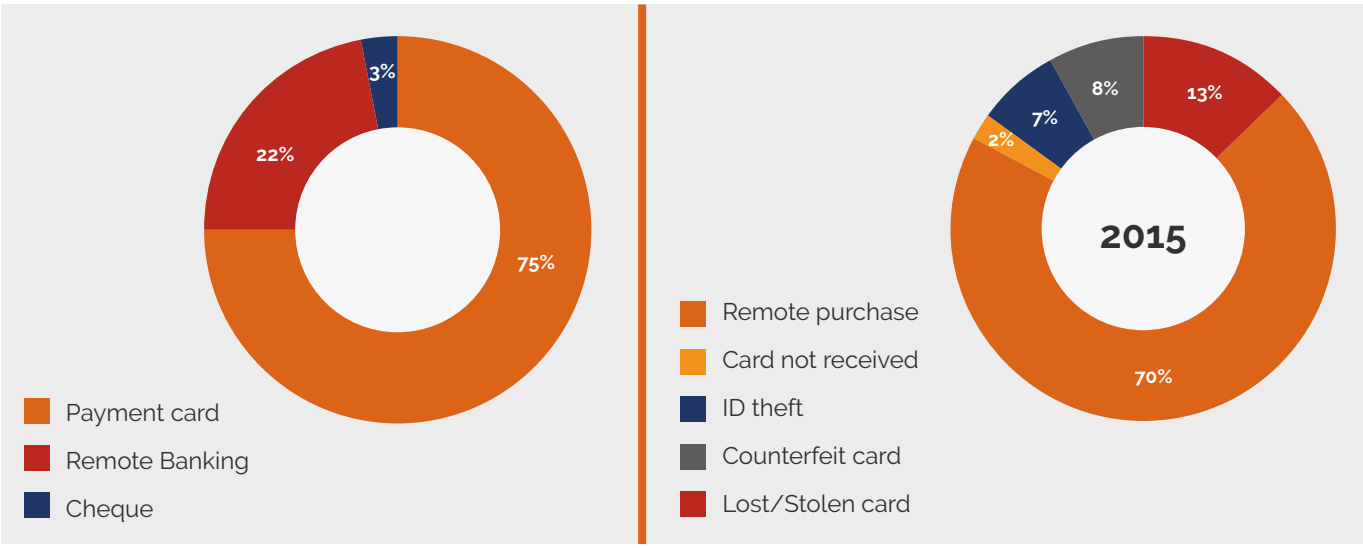
The client is looking to expand the use of the transaction monitoring system to other payments channels, including point of sale and online (digital). Beyond combating fraud, the group is looking at leveraging our solution for performance optimisation, improving uptime and availability and enhancing customer experience. It is also considering combining the Gyrus operational management platform and analytics functionality to improve the customer experience.

TODAY'S THREATS DEMAND A MORE PROACTIVE APPROACH TO PAYMENTS SECURITY

Any security breach in a financial institution's payments environment—no matter the scale—represents a massive business risk. Proactive monitoring and management of financial transactions significantly reduces this risk.

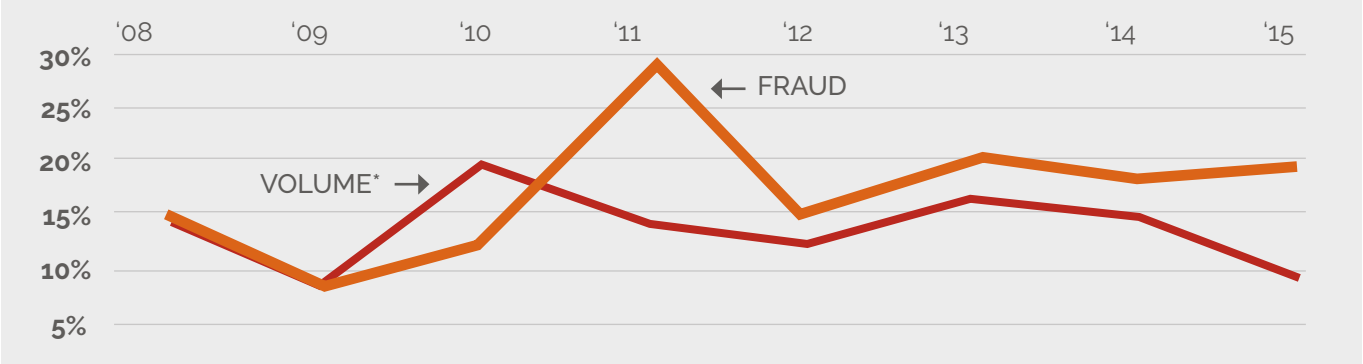
The fraud and information security risks facing the financial services industry are constantly growing in scale and sophistication as global crime syndicates focus their considerable resources on the lucrative new opportunities that cybercrime offers. This type of cyber crime is determined and professional, using a blend of custom malware, card skimming, social engineering and coordinated attacks to bypass the traditional defences in payments systems.

TOTAL 2015 FINANCIAL FRAUD LOSSES BY TYPE



Source
Financial Fraud Action Report – UK

GROWTH IN FRAUD VS. TOTAL CARD VOLUME WORLDWIDE



Source
© 2016 The Nilson Report

PAYMENT CARD FRAUD 2015

Source
Nilson Report

Today's cutting-edge man-in-the-middle attacks, for example, are designed to bypass the usual authentication methods to gain access to users' bank accounts or to carry out real-time transactions. The most advanced attacks could see fraudsters steal millions of dollars in a few minutes before most fraud monitoring tools pick up the anomalous nature of the transactions.

Fighting the new generation of advanced persistent threats demands an innovative approach that closes the network blind spots and payments systems vulnerabilities exploited by cyber crime syndicates. Real-time, transaction-level monitoring tools have an invaluable role to play here as a trusted, reliable source of quality transaction data.

They provide financial services institutions and payments companies with a real-time, end-to-end operations view into the performance of digital banking transactions within their omni-channel banking, self-service networks and payment processing environments. This software is increasingly being used to bridge IT operations performance, card operations and fraud prevention.

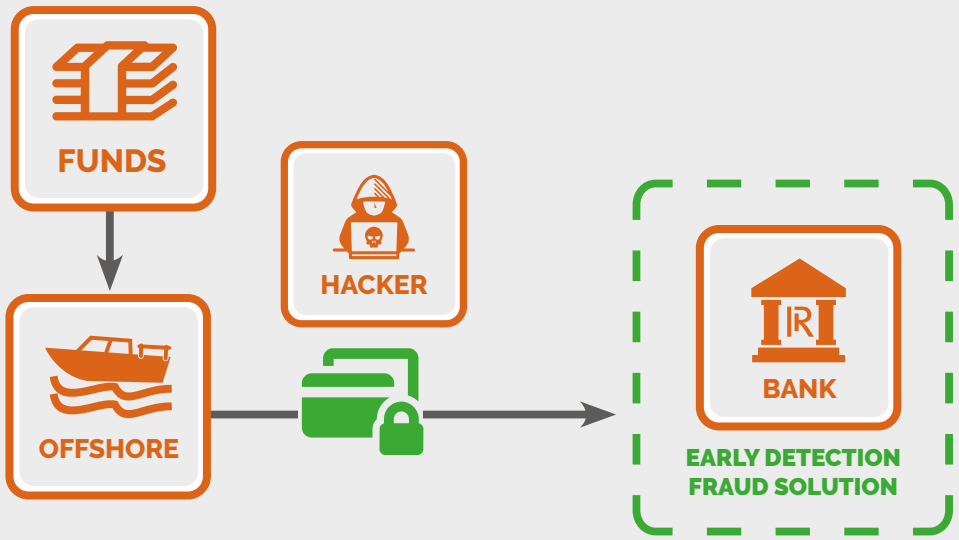
MONITORING PAYMENTS TRANSACTIONS IN REAL-TIME TO IDENTIFY ANOMALIES

Risk monitoring systems in the back-end of payments infrastructure cannot easily detect attacks on front-end devices. A robust transaction monitoring system can help organisations to identify anomalies by matching front-end and back-end transactions.

A modern, real-time transaction monitoring solution can complement an organisation's existing fraud detection systems by adding a new forward layer of defence against transactions that might otherwise fly beneath the radar. Such a solution enables an organisation to capture and correlate the complete data flow of every transaction, allowing card operations and fraud prevention teams to see when transaction messages and data flows have been altered or tampered with.

Early Detection Fraud Solution

By implementing Stanchion's early detection fraud solution – the front-end and back-end of your payments system are reconciled in real time allowing you to identify anomalies and potential threats instantly.



The platform can forward real-time alerts about anomalous transactions to the enterprise's existing security information and event management or terminal and device management system. The ops and security teams will have accurate and consistent data on hand for analysis and action.

Security-related transaction message fields and metadata include:

- Message types
- Card numbers
- Amounts
- Transaction dates and times
- Fraud response codes
- Terminal ID's
- ISO 8583 messages

Anomalies detected include:

- Fake processing due to switch malware and card compromises
- Isolation of ATMs or POS terminals used in coordinated attacks
- Cards being used several times in rapid succession at an ATM or point of sale
- Unexpected EMV fall-backs
- ATM cash-outs due to foreign or high-value card usage
- Transactions entering a payments switch, but never leaving for authorisation

USE CASES

Catch compromised cards before crime syndicates do too much damage
Once fraudsters have skimmed a card, they'll be racing to use it for as many transactions as possible before it gets added to the hot list. Transaction monitoring software will flag the use of a card for an unusual amount of transactions in a row, coordinated across multiple devices. The fraud team can set thresholds based on variables such as card type, transaction values and location to minimise false positives.

Detect unusual activity at terminals
Transaction monitoring can detect anomalous transactions at terminal level immediately so suspect terminals can be investigated. Thresholds can be based on terminal type, manufacturer and location to detect rapid, repeat transactions, fall-backs to magstripe at EMV-capable terminals, excessive reversals and transactions occurring outside normal business hours.

Identify compromised devices
Some crime syndicates use targeted malware to get payment switches to authorise transactions locally, instead of dispatching them to back-end fraud and authorisation systems for evaluation. This malware is often designed to support card skimming or coordinated withdrawal attacks. A sophisticated solution will track transactions at the network level and look for transaction requests that enter the switch, but never exit into back-end systems.

MANAGE YOUR RISK WITH STANCHION

We are helping leading financial services clients to implement solutions that enable them to stay ahead of a fast-changing threat landscape. As a trusted, innovative partner with a global footprint, we have the technology, expertise and support to ensure high performance, availability and total system integrity in any global financial institution's payments environment.

TOP CONTROL PRIORITIES OF BANKS

66%
Meeting regulatory compliance and reporting standards

54%
Improving risk management

Source
Global banking outlook survey – EY http://www.ey.com/Publication/vwLUAssets/EY-global-banking-outlook-2017/$FILE/EY-global-banking-outlook-2017.pdf

69%
Managing reputational risk, including conduct and culture risks

64%
Enhancing cybersecurity/data security

Source
Global banking outlook survey – EY http://www.ey.com/Publication/vwLUAssets/EY-global-banking-outlook-2017/$FILE/EY-global-banking-outlook-2017.pdf

ABOUT STANCHION

Founded in 2001, with offices globally, Stanchion provides a complete range of FinTech related solutions recognised for consistently delivering high performance and total system integrity across complex payments environments. With a global team of more than 100 specialists, Stanchion has collaborated with high profile clients from retailers, banks, credit unions, card schemes, payment processors and payment systems around the world.

www.stanchionpayments.com