› Solution Brief

Business Impact

"Managing fraud across an enterprise entails understanding customer behavior as well as analyzing transactional activity within the context of all delivery channels – both are necessary to have a true view of what is happening in a specific customer's accounts."

Enterprise Fraud Management, Aite Group LLC, May 2014

Challenges

- Many data silos make it difficult to gain a holistic view of session behavior, allowing fraudulent payments to slip by.
- In isolation, financial transaction anomaly detection approaches can be highly inaccurate, generating a large number of false-positive alerts that can overwhelm resources.
- With commercial account takeover it can be difficult to find the rare fraud events that represent potentially large fraud losses per transaction – so you can act on them in real time.
- Higher false-positive rates negatively affect the customer experience and your organization's reputation.

Reduce online fraud losses while minimizing impact to customer experience

With the onslaught of organized cybercrime and a payment landscape shifting to digital currency, online data breaches are escalating to new heights, with no sign of slowing down. Take the growing volume of smaller payment transactions, card authorizations and registrations on millions of mobile devices, and it's clear that financial institutions need to beef up their defenses – and fast – to get ahead of the game.

Millions of dollars of revenue are lost to online fraud each year, not to mention the impact on organizational reputations. But perhaps most importantly, your lifeline – customer satisfaction – can be severely affected by declining transactions prompted by false-positive alerts.

You've got stacks of data that you can't connect and associate, teams of fraud analysts and an avalanche of alerts. With the sophistication and velocity of attacks, you need a way to look across all those sources of data at once to correlate events. You also need big data analytics and machine learning at warp speed to identify the highest priority alerts and threats in real time to decide which alerts warrant action.

Along with data management, SAS delivers a layer above operational systems that provides situational awareness to help zero in on potential flash attacks. Our automated, real-time, behavioral and predictive analytics gives you the power to spot trends and emerging risks. With SAS®, you can identify attacks faster and reduce your risk exposure.

Our Approach

SAS offers an enterprise approach to data aggregation and real-time fraud detection to reduce false positives, detect risks early, minimize disruption to the customer experience, and protect institutional reputation.

- **Gain a holistic view of data and events.** A single IT platform acts as a staging area to aggregate data and risk measures from multiple systems. Gain a consistent view of payments and session risks, correlate events, and triage high-risk scores and alerts. Screen payments with minimal customer disruption using session and device insight and transactional data. Authenticate sessions in real time, and make intelligent use of relevant third-party data to halt an online session prior to exfiltration.
- **Apply advanced analytics to predict rare and risky fraud events.** Unlike sampling, SAS monitors 100 percent of transaction activity (not just financial) to act on early indicators. Using behavioral analytics combined with our machine learning lets you reduce the noise and more accurately detect fraud in real time.
- **Accurately detect fraud to reduce customer annoyance.** Protect customers with a real-time system that reduces false positives and customer disruptions. Self-learning models adapt to changing patterns in behavior and contextual awareness that capture events, failed authentication, behavioral abnormalities, early risk behaviors and how customers are using products across the organization.

sas
THE POWER TO KNOW.

The SAS® Difference:

- **An enterprise approach**. SAS data aggregation, combined with advanced analytics and machine learning, provides a comprehensive approach to detect a multitude of cyber vectors. Bring third-party event data with other information about your customers in other products and channels together to gain a holistic view of customer activity. A staging area delivers a single fraud management solution that scores and triages alerts from multiple systems. SAS is multitenancy with the ability to have a single solution controlled by different parts of your business. All data comes into a single point, but user accessibility is based on specific needs of the business. Plus, users don't need programming skills.
- **A variety of advanced analytical tools for fraud analysts**. To support more accurate behavioral analytics, SAS offers statistical and predictive models, rule engines and entity link analysis. Self-learning models adapt to changing patterns in behavior; for example, unsupervised learning, predictive modeling, anomaly detection, etc. With SAS, you can achieve value detection rates (VDR)* as much as 60 percent using our models over and above that provided by business rules alone or in comparison to other industry modeling techniques.
- **Patented behavioral analysis to accurately identify suspicious behavior**. SAS captures customer behavior patterns from every source and evaluates that contextual information every time a transaction is scored, helping you understand how customers transact and even how they conduct their relationships with your bank through electronic and mobile channels. For example, uncover suspicious activity based on behavior at the customer, account and device level.
- **Real-time scoring, decisions and authorization**. Using business rules, any transaction can be treated in a number of ways to influence decisions back to the authorization system. This triggers further authentication to approve, decline or refer – in real time – so that you can catch fraud as it occurs and avoid bothering your customer.

* VDR is a proportion of fraud detected by the system out of the total fraud.

Case Study

In its ACH and wire transactions, a large commercial bank was incurring losses through email compromise and malware attacks. These low-volume attacks were hard to detect, but high value and high risk to the bank due to their effect on customer experience. Its rules-only approach wasn't finding the subtle differences between normal and abnormal behavior. The bank needed to modernize its current infrastructure to support an enterprise approach and use advanced analytics to detect out-of-character behavior that might indicate suspicious activity. It also wanted to include session and device data with customer transaction information for decision making.

Solution

SAS delivered a fraud solution for intraday deployment of business rules and application of advanced neural network and machine-learning models. The bank now has anomaly detection techniques for identifying abnormal behavior and the ability to recognize suspicious payments within batch files.

Results

- Improved prevention of commercial account takeover.
- Prevention of high-value losses.
- Reduction in staff to mitigate ACH/wire fraud risks.
- Case detection rate increase to 70 percent for wire and 60 percent VDR for all wire fraud, while preventing 60 percent of total losses.

What if you could …

Combine various e-commerce and m-commerce events and risk measures from multiple systems to have a consistent view of customer and session risk?

Get a complete understanding of each customer's normal pattern of session behavior?

Prioritize and assign resources to potentially fraudulent cases based on workload and skill set?

Predict the likelihood that a transaction would be fraudulent and stop fraudulent payments as they occur and before they're approved?

Prevent fraud on customer accounts before they notice?

Provide a frictionless customer experience while safeguarding the bank's assets and maintaining client trust?

You can. SAS gives you THE POWER TO KNOW®.

SAS Facts

- 93 of the top 100 companies on the 2014 Fortune Global 500® are SAS customers.
- SAS was recognized as a leader in the *Chartis RiskTech Quadrant for Financial Crime Risk Management Systems 2014* (Jan. 19, 2015).
- SAS was recognized as a leader in "The Forrester Wave™: Enterprise Fraud Management, Q1 2013."

Learn more about SAS software and services for fraud at sas.com/securityintelligence.

THE POWER TO KNOW®