Reduce payment fraud losses while lowering associated costs

Business Impact

"Motivated by the growing use of digital banking and payments, criminals are targeting institutions' websites, consumers' digital devices and non-bank accounts, and any other avenues that allow them to compromise data and monetize identities. Worse still, there are now too many digital vulnerabilities for an FI to manage alone, fraudsters are becoming more sophisticated with every day that passes, and consumers are increasingly looking for help to feel safe from identity crimes."

2018 Fraud and Security Trends, Javelin Strategy

Challenges

- **Insufficient fraud detection systems**. Rules-based systems flag too many legitimate customers; fraudsters discover ways to circumvent the system.
- **Lack of predictive abilities**. Rules-based systems can't identify the future likelihood of fraudulent activity.
- **High costs of doing business**. Operational, customer and reputational costs rise with too many false positives, inefficient investigative processes and lack of speed in transaction authentication.
- **Organizational complexity**. Electronic banking, multiple portfolios and related business lines across channels are all growing to create a more complex matrix of offerings.

The Issue

There's a dynamic payment landscape taking shape with the global growth of digital payments and emerging new payment methods (e.g., mobile apps, blockchain). With all these avenues of money transfer, perpetrators are continuously finding creative ways to outsmart fraud detection systems by uncovering points of exposure in payment offerings. As these emerging methods become the channels of choice, banks must adopt effective fraud detection and prevention strategies – and fast.

Large losses occur each year due to payment fraud, adversely impacting corporate reputations. But perhaps most importantly, the barometer of success and continued revenue generation – customer satisfaction – can be severely affected by incorrectly declined transactions prompted by high false positive rates. With the sophistication and velocity of attacks, you need a way to correlate events and quickly apply machine learning to identify the greatest threats in real time so you can decide which alerts warrant action.

The SAS® Approach

- **Bolster data integration and handle higher data volumes**. Connect siloed data sources regardless of format. Deliver faster results from increasing volumes of data by utilizing distributed environments (such as Hadoop), which are critical to fraud assessment.
- **Better monitor the behavior of individuals to detect fraud**. Reduce false positives by using data across each customer account and transaction for higher accuracy at the account, customer and product levels.
- **Monitor 100 percent in real time**. Integrate with payment systems real time by scoring 100 percent of all transactions. Monitor new relationships to detect subtle patterns of behavior, prioritize suspicious cases and predict future risks using advanced analytics.
- **Apply machine learning continuous improvement**. Assess new machine learning algorithms and analytics using champion-challenger evaluation, as well as simulation and estimation, to confirm the benefit of guided rule development.
- **Improve operational efficiency**. Perform interactive queries and generate reports with web-based data visualization. Measure anti-fraud program performance by defining and monitoring KPIs via a dashboard environment.

The SAS® Difference

SAS solutions let you develop a cohesive strategy for control, discovery, prioritization and deterrence. Only SAS provides the highest level of fraud protection through:

- **Data integration** that handles a vast range of data formats across financial institution and third-party vendor systems. This includes a flexible message layout (API) that describes all transactions according to who was involved, type of activity, where the transaction originated, and how the transaction was authenticated.
- **Detection and alert-generation** tools offering multiple analytic techniques, so you can:
  - Capture all payment behavior from all sources via a unique patented signature technology.
  - Score and decision 100 percent of transactions.
  - Detect abnormal patterns that may indicate previously unknown fraud and anomaly detection for identification of future threats.
- **Fraud network analysis** for going beyond individual views to analyze all related activities and relationships at a network dimension so you can uncover previously hidden linkages that would otherwise go undetected.
- **Case management** capabilities systematically facilitate investigations and enable the capture and display of all pertinent information, either via your existing case management system or the enterprise case management system offered by SAS.
- **Alert triage management** that provides business process management for external systems.

Case Study

PKO Bank Polski

Situation

PKO Bank Polski wanted a solution that could scale with the bank's growth, including the ability to handle ever-increasing volumes of transactions and data.

Solution

SAS provided the bank with an enterprise platform that covered all fraud typologies, including application monitoring, to increase efficiencies and improve detection.

Results

PKO Bank Polski was able to reduce losses by achieving higher levels of fraud prevention and fine-tuning false positives and negatives. It also strengthened the bank's reputation for customer security in its local market, and is now viewed as a leader in customer journey improvement.

What if you could ...

Improve customer service

What if you could maintain the same level of monetary fraud prevention while simultaneously improving the customer experience by lowering false positives as much as 75 percent?

Quickly capture changes in behavior that may indicate fraud

What if you could create unique customer signatures using variables from application, bureau, negative-file, derived-value and cross-product data at account, customer, product and network levels?

Score transactions in real time

What if you could score all transactions in real time to determine whether to accept, reject or defer payment to help prevent fraud at points of sale before the money has exited the account?

Adapt strategies to regional practices

What if you had the ability to easily configure and adapt your fraud strategies to regional business practices and your bank's specific needs?

SAS Facts

- SAS customers make up 96 percent of banks in the Fortune Global 500®.
- Over 90 percent of the top 100 global banks use SAS.
- More than 3,100 financial institutions worldwide are SAS customers.
- SAS has more than four decades of experience working with financial institutions all over the world.

Learn more at sas.com/securityintelligence.

To contact your local SAS office, please visit: sas.com/offices