WHITE PAPER

Customer Experience: The Flip Side of the Fraud Detection Coin

Addressing deposit fraud while ensuring high-quality customer experiences

Contents

Balancing Safety With Service Quality

For traditional banks, competing in an increasingly digital business environment is a challenge. And it's getting tougher on several fronts.

First, today's digitally oriented customers expect banks to provide an ever-higher quality experience defined by speed and the flexibility to conduct business across many channels. They've grown accustomed to going online and transferring money between accounts, for example, and using their mobile device to make payments and check their account balance. These kinds of experiences have raised the bar in terms of customer expectations – and banks need to keep up, or risk losing customers. This is particularly true of millennial customers, as they have little regard for loyalty, which banks have traditionally relied on to build their business. Once frustrated by inconvenience, they don't hesitate to switch banks – and thanks to the internet, this is now a fast, painless process.

At the same time, banks need to protect themselves and their customers from sophisticated fraudsters who are constantly innovating in response to the latest regulations and detection methods. New Europay, MasterCard and Visa requirements, for example, are making it difficult to create counterfeit cards for fraudulent use. So many fraudsters are switching gears, collecting customer data needed to create new bank accounts and lines of credit through online banking forms. The anonymity of the modern account creation process – a concession made by banks to meet customer demand for speed and convenience – makes it all too easy for them to open hundreds and even thousands of new accounts using stolen customer data.

Despite the scale and intensity of fraud threats today, banks can't afford to simply batten down the hatches and brace themselves until the storm passes, notes Javelin Research. According to their recent mobile digital finance study, "Consumers have become discontented with a financial pace that lags behind the rest of their digital lives."[1] Millennials, in particular, are digital natives who now expect real-time responses and information from just about every organization they interact with. And their bank is no exception. Whether it be opening a new account, extending a loan, providing investment assistance or depositing a check, they want a fast, hassle-free process.

According to their recent mobile digital finance study, "Consumers have become discontented with a financial pace that lags behind the rest of their digital lives."

As noted by Javelin, these trends have resulted in a push by banks to accelerate consumers' access to their money in a variety of areas, including:

- Credit (real-time credit line approval and immediate access upon approval).
- Mobile remote deposit capture (mRDC).
- Same-day ACH (automated clearing house) payments.[2]

But it's critical that banks balance meeting customer expectations regarding speed with the potential risk of a given transaction. Making it excessively difficult for an honest customer to perform an honest transaction (friction) will result in poor customer satisfaction, while a lack of sufficient consideration for the risks involved in the activity may leave the financial institution in a position of financial exposure or loss.

[1] *Taking the Risk Out of Convenience: Javelin research on the threats associated with mobile digital finance, and what to do about them*, August 2016, SAS

[2] Ibid

Deposits: The Latest Battleground for the Customer Experience

This dilemma is particularly evident in the management of deposits. In the minds of customers, it's all very simple; just stop every bad deposit and approve every good one – because they want access to their deposits as quickly as possible, preferably immediately.

But in reality, banks must find the delicate balance between letting these transactions process unencumbered (so that customers aren't frustrated by delayed access to their money) and doing the right level of diligence to detect and prevent fraudulent activity.

And the risks are real and growing. According to the *2015 ABA Deposit Account Fraud Survey*, which examines the leading threats against deposit accounts, current and projected fraud losses, and other fraud-related topics:

- Fraud against bank deposit accounts cost the industry nearly $2 billion in losses in 2014, according to ABA estimates.
- Debit card fraud – signature, PIN and ATM combined – accounted for 66 percent of industry losses, followed by check fraud at 32 percent. The remaining 2 percent of losses were attributable to online banking/electronic transactions such as wire and ACH.
- In addition to the estimated fraud loss amount, banks' prevention measures stopped another $11 billion in fraudulent transactions.
- Respondents cited "increase in fraud attempts" as the primary driver for higher Demand Deposit Account (DDA) fraud losses in 2014 compared to 2013. Other factors mentioned included banks' move to more customer-friendly policies on funds availability, new channel/product offerings, and growth in banks' deposit account base.
- The leading check fraud categories were counterfeit checks and return deposited items (RDIs).[3]

But as an executive at a large regional bank explained to SAS, "Not all return deposit items result in overdraft or loss." If a bank is scoring all deposits for risk, they will find some with a higher propensity to be fraudulent, while other, similar transactions will be legitimate. So it doesn't make sense to block ***all*** deposit transactions having similar characteristics. Banks just need a way to assess whether the risk of allowing early access to some deposits is worth it, and when it's not. This means thinking through questions such as:

"Not all return deposit items result in overdraft or loss." If a bank is scoring all deposits for risk, they will find some with a higher propensity to be fraudulent, while other, similar transactions will be legitimate.

- How many false positives are acceptable?
- What false-positive ratio is acceptable to both banks and their customers from a quality-of-service perspective?
- How can banks use what they know about each customer to make personalized, insight-based determinations about the risk of their deposits (for example, for small checks? Or large checks from a long-term, stable employer versus a net-new, unknown source)?

[3] 2015 ABA Deposit Account Fraud Survey, American Bankers Association, 2015

As explored in this paper, what banks need is a new approach to deposit risk monitoring and risk assessment – one that is data-driven and analytical. And one that turns diverse customer data into real-time fraud and risk insights that can be used to make swift, optimal decisions regarding deposit funds availability.

Automating and Accelerating Deposit Fraud Detection and Risk Monitoring

To optimally balance deposit risk with quality of service, banks need an integrated risk data infrastructure that enables them to collect customer data, including behavior data; integrate it with transaction data to analyze it and measure exposure and risk for each deposit; and make fast, automated, risk-weighted decisions regarding speed of funds availability.

> To optimally balance deposit risk with quality of service, banks need an integrated risk data infrastructure that enables them to collect customer data, including behavior data.

For example, SAS delivers a fraud infrastructure with solutions that:

- Enhance information credibility by integrating disparate data sources regardless of format, and applying data quality techniques to ensure accuracy.
- Analyze large volumes of structured and unstructured data quickly and efficiently.
- Effectively monitor the behavior of individuals to incrementally detect fraud and reduce false positives by using data across all of a customer's accounts and transactions to generate more accurate profiles at the account, customer and product levels.
- Find deposit fraud faster with real-time integration to authorization systems and on-demand scoring of 100 percent of purchase, payments and nonmonetary transactions.
- Uncover hidden relationships, detect subtle patterns of behavior, prioritize suspicious cases and predict future risks using advanced analytics – including champion-challenger, simulation, estimation and unlimited rule-writing capabilities.
- Automatically generate recommended actions for each deposit – based on available data – so that customers gain access to funds as quickly as possible.
- Improve investigator efficiency with web-based data visualization to perform interactive queries, generate reports, and understand how to improve data models.
- Measure anti-fraud program performance by defining and monitoring KPIs via a dashboard environment.
- Deliver faster results from increasing volumes of data by utilizing distributed environments.

Analytics at Work: Proving the Value

Let's take a look at how one SAS customer is using SAS software to address deposit risk while optimizing customer experiences. In this case, this large, regional full-service retail bank with approximately $75 billion in assets and over 700 branches was struggling to balance fraud risk and customer experience quality related to deposit activity.

Lack of Real-Time Monitoring of Deposit Transactions

At this bank, customers could make deposits at branches as early as 8 a.m. But these transactions were not posted and analyzed for fraud until late that evening or early the next morning.

For years, the bank had used an industry-standard deposit fraud software solution that analyzed deposit transactions in a batch environment each day; alerts were available for analyst review the morning after each transaction took place. So risk monitoring was not real-time – resolutions of a deposit transaction alert were delayed by as much as 24 hours. This was a serious issue, as many times – especially for alerts worked later in the day – fraudsters would have removed the funds before a hold could be placed on them.

Given the delay in fraud detection, the bank relied heavily upon tellers to report suspicious deposit activity at time of deposit. Management wanted to move monitoring and decision making from "next day" to the actual day and time of deposit, and thus eliminate reliance on tellers to report suspicious deposit activity.

Using real-time, data-driven insights into risk, the bank could take a proactive approach to monitoring deposit activity that would reduce fraud exposure to the bank and/or the customers and address issues related to:

- **The customer experience and earlier funds availability**. Management wanted to make deposited funds available to customers sooner than the next day, especially for those customers with a long and strong relationship with the bank. To do this, they needed an informed way to differentiate how they treated various customers, but the alert generation process failed to take into consideration the customer relationship.
- **High false-positive rates**. The bank was using limited rules and data in its deposit transaction analysis along with a high volume of teller referrals, which resulted in a very high false-positive rate (150:1 to 200:1 false positives.) This, in turn, resulted in frustrated customers and significant resource challenges when dispositioning the numerous alerts and referrals.
- **Limited flexibility of their existing system**. The bank's existing fraud detection system provided a limited number of parameter settings, which resulted in less flexibility to make adjustments that would maximize alert quality and stratify alert assignment and priority.
- **Desire for expanded information for analysis**. Management wanted to utilize a broader set of data in their deposit fraud analysis, including information about the customer's overall relationship with the bank.

Using real-time, data-driven insights into risk, the bank could take a proactive approach to monitoring deposit activity that would reduce fraud exposure to the bank and/or the customers and address issues.

- **Lack of flexibility in alert prioritization and assignment**. The bank's existing solution provided minimal flexibility around alert prioritization and alert assignment, as alerts were generated as paper reports. They wanted a way to prioritize alerts based on rule(s) violations, dollar amounts, customer relationship and more.
- **Cumbersome paper reports and lack of a feedback loop**. Analysts had to record their review and disposition of alerts on paper reports, which made aggregating data and building reports a time-consuming and cumbersome process, hindering timely analysis of critical information to detect fraud. The bank wanted a system that:
  - Enabled efficient access and analysis of transaction and disposition data.
  - Allowed faster investigation of deposit alerts.
  - Provided the ability to record the recommended action right within the system.

  Furthermore, all captured review and disposition data wasn't serving a purpose of optimizing the quality of future alerts generated via a feedback loop to continuously optimize fraud detection models. Together, the tenets of a non-paper and feedback approach would pave the way for easier analysis and ensure the accuracy of the funds availability hold decisions made by the solution or an analyst.

By addressing these issues with the right solution, the bank believed it could improve the customer experience by making more deposited funds available to customers sooner – even at the time of deposit – without increasing the risk of fraud exposure and loss to the bank or the customer. To operationalize their plan, they chose to deploy SAS fraud solutions, which can perform rapid data analysis and automate decisions regarding funds availability holds on deposit activity. The result? Earlier funds availability **and** lower deposit fraud losses.

The Existing Environment

Prior to deploying SAS fraud solutions, the bank used an industry-standard, rules-based deposit fraud software solution. To detect fraud, it analyzed a limited amount of transaction data and only minimal customer data such as name, account number and account open date. The length, depth and nature of the relationship the customer had with the bank was largely disregarded, so many of the deposits and deposit items of customers with lengthy and extensive bank relationships were incorrectly slated for mandatory, manual review slowing funds availability. In addition, fraud analysis occurred one time per day early in the morning **after** the posting of deposit transactions. Results from this analysis were published as a paper report of alerts and related transaction data, which were then worked from 7 a.m. to approximately 3 p.m. each day.

Because of the delays created by the batch processing of deposit transactions, the bank relied upon tellers to refer highly suspicious deposit transactions to the Deposit Fraud team for a manual review at time of deposit. These transactions were reviewed more quickly, with holds placed where appropriate. Between the teller referrals and the alerts generated by the existing deposit fraud analysis solution, the bank generated a significant volume of work to review and disposition; given this volume, they would have needed 24 FTEs to complete it in a timely manner, but the department was only staffed with 12.

The Business Case for SAS® Fraud Solutions

After evaluating various solutions, the bank ultimately selected SAS software to address its deposit fraud detection challenges. SAS is a proven name in the fraud and risk landscape of the banking industry with a proven real-time fraud solution. It's also the leader in the decision science and data analytics field and could work hand in hand with the bank to optimize the solution. Finally, SAS has a core competency in data management, which is critical to the bank's success, as large volumes of data would need to be retrieved from numerous banking systems.

The bank's business case for this investment showed how it would provide a return on investment that aligned with corporate goals, including savings through:

- Elimination of current software licenses.
- Reduced false-positive and false-negative results.
- Operational efficiency gains (for example, by reducing alert volumes and eliminating manual processes).

Deploying SAS® Fraud Solutions

SAS fraud solutions for deposit monitoring were implemented in three stages, each aligned with a deposit method: mobile (remote deposit capture), ATM and teller. The solution is used in real-time situations using two basic sets of rules: 1) rules created at the time of the solution implementation, and 2) rules created after production to address specific trends and situations arising after initial implementation. Together, these rules generate a 60 percent false-positive rate as it is measured between alerts generated and RDIs, while the more specific situational rules generate a 45 percent false-positive rate.

The solution takes one of three actions upon each deposit item reviewed:

- The transaction is analyzed, and no hold action is required based on the SAS solution's review.
- The transaction results in a hold recommendation made by the SAS solution and communicates to the bank's core processing system. (Holds are often placed due to the existence of early warning system [EWS] hard hits and/or violations of one of the post-implementation rules.) All holds placed automatically by SAS are reviewed to ensure that holds were not placed on special items that Reg CC mandates timely funds availability.
- The transaction is out-sorted to a queue for manual review and disposition.

The deposit method determines whether a transaction is analyzed in real time or not. Mobile deposits are analyzed in real time prior to item processing. This may result in the review of an erroneously entered transaction amount whether by error or intentionally. Teller, commercial and ATM deposits go through item processing and are balanced, eliminating this potential issue.

Alerts and Queues

Alerts are presented in four priority queues based on specific characteristics of the deposit transaction. Alerts are generated on an item-level basis. In situations where an account-level rule is utilized, the alert is generated on the item that triggers the rule. In situations where multiple rules are triggered on an item, the alert is placed in the queue relative to the highest-priority rule violated.

Analysts are not assigned to a specific queue. All analysts work Priority 1 alerts until they are completed and then move to the next queue. As new Priority 1 alerts are generated, they are worked by the available analysts.

Alert Details

A portion of the alert information provided by the SAS solution is a document image number. This number allows the analyst working on an alert to retrieve and view deposit items, as well as see other items drawn on the same bank and account number that have been deposited into other accounts within the bank. Image viewing capability is a critical piece of the alert review process and enables analysts to work efficiently, with an average of 22 alerts per hour.

Reporting and Decision Making

The bank maintains monthly reporting by individual rule, including:

- Number of alerts generated.
- Number of holds placed.
- Number of items returned.
- Quality statistics:
  - Alerts to holds percent.
  - Holds to RDIs percent.

In addition to these statistics, the bank tracks whether an RDI results in an overdraft and how long the overdraft remains in place. As one bank manager stated, "Not all RDIs result in overdraft or result in loss. Many are on good, long-term customers that present minimal risk of loss, and the customer service aspect of not holding the item far outweighs the risk."

The Results

With the SAS fraud solutions in production, the bank realized a number of benefits, including:

- **Reduced deposit fraud losses**. Annual losses from deposit fraud at the bank were reduced by $1.6 million in the first year.
- **Reduced alert volume**. Overall, alert volume was reduced by 51 percent between the first six months in production and the six-month period just prior to SAS fraud solutions going live in production.
- **Fewer false positives**. The false-positive rate on alerts was reduced 43 percent in the first year of production compared to the same time period the year prior. False-positive rates went from between 150:1 and 200:1 down to 35:1, not counting the impact of EWS, which further reduced the false-positive rate to approximately 12:1.

- **Reduced funds availability hold volume**. Funds availability holds were reduced by 31 percent; at the same time, deposit transaction volume increased 26 percent.
- **Fewer EWS inquiries**. Enhanced analytics provided by SAS reduced the need to inquire upon deposit items with EWS. In addition, the real-time EWS inquiry was initiated at the time of the implementation of the SAS solution.
- **Hold placement automation and notification**. The placement of holds within the core banking system went from being a manual process involving the entering of detailed account, customer and item information to an automated feed of information from SAS fraud solutions. Automation reduced manual process time and the potential for entry errors. In addition, hold notifications, which used to be printed by the bank and mailed to the customer, are now automated using an API between SAS solutions and the printer.
- **Reduced reliance on front-line intervention**. The bank no longer needs to rely on the front-line tellers to notify the fraud department of suspicious deposit activity. Now, they can use SAS fraud analytics solutions at the time of deposit to assess risk, which reduced referrals from the line by over 95 percent (specifically, from 1,500-2,000 a day to approximately 15 a day). This reduction in teller referrals saved the tellers a great deal of time, allowing them to handle more customers without delay.
- **Elimination of paper reports and manual reporting processes**. Using SAS fraud solutions, analysts can view alert information and record alert dispositions within the fraud solution, eliminating the need to print alert reports. Furthermore, manual reporting has been replaced by an automated process, as SAS fraud solutions simply pull the latest alert information and disposition information stored within its database. The existence of deposit transaction, alert and disposition information within the SAS solution enables much easier analysis, which can be used to refine the quality of alerts generated and the accuracy of the holds placed. And historical data contributes to a feedback loop to optimize future fraud detection.

Realizing the Benefits

As this customer example illustrates, banks using SAS fraud solutions – in conjunction with expanded data sets that provide insights into the customer relationship – can deliver significant benefits such as:

- Faster processing of deposits and transfers.
- Greater sensitivity and responsiveness to customer needs.
- Higher customer satisfaction.
- Increased customer retention.
- Reduced complaints.
- Reduced false positives and false negatives.
- Increased operational efficiency.

These benefits should be included in any business case used to justify the implementation of an analytic solution for deposit fraud.

Learn More

Read more about SAS solutions for fraud and security intelligence at: sas.com/securityintelligence.

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