FLYING PHASE

Reducing Risk, Lowering Cost in Credit Card Authorization Decisions

CAPABILITIES COVERED

Credit

Reporting Automation

Business Analytics

Process Improvement

FEATURED CONSULTANT

Kevin Baquero

THE SITUATION

The credit card tech team at a Top 10 bank was concerned about the organization's exposure to risk stemming from how it authorized credit card transactions. Of the more than seven billion transactions the bank processed each year – twenty million each day in real-time – two million of those were processed and decisioned with incomplete information by the in-house card authorizations platform. Despite having already invested heavily to create an authorization platform – one with a resilient, robust infrastructure – the bank decided an additional $1.2M was necessary to bolster the platform's structure for improved stability across its internal decisioning processes.

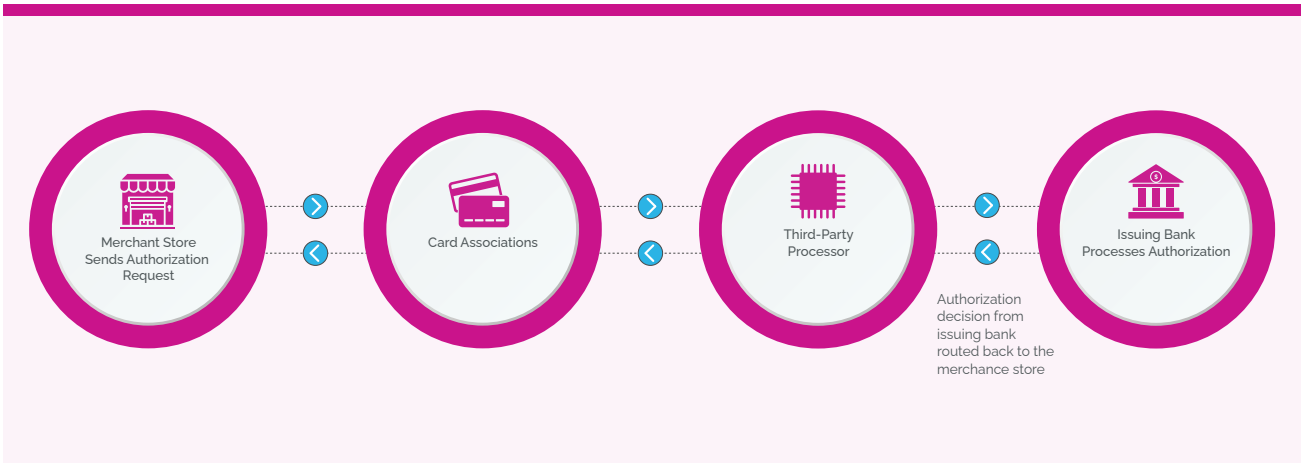

Figure 1: Decision Authorization Loop

The Decision Authorization Loop (Figure 1) shows how a credit card transaction works. Every time customers swipe, insert, or tap their credit card, the bank receives an authorization request from the card associations – for example, Visa and MasterCard – and the third-party credit card processor. When that request comes in, the bank's authorization platform decides whether to approve or decline the transaction.

As Bank Internal Authorization Process (Figure 2) illustrates, the issuing bank's platform does this by using three distinct modules to conduct three separate but simultaneous decisions that assess fraud, credit-risk, and customer account preferences. Under perfect conditions, each of the three modules would make a decision and return it to the platform's central decision module. This central module would generate a final decision to approve or decline a transaction and then relay that decision back to the merchant store by way of the third-party credit card processor and card associations.

To provide credit card users with an optimal experience, the bank was required to respond to the third-party processor within 500 milliseconds (a half second) for each authorization. If the bank failed to respond within the allotted time, the third-party processor would make the authorization decision on its behalf and then charge a per-authorization penalty fee.

The volume of decisions that needed to be authorized and the limitations of the system tending to that process, from cloud-service degradation to missing data, led to one or more of the three in-house modules failing to provide a response time to the central module that met the half-second requirement. To avoid contractual penalties for failing to respond in time, the bank's in-house platform would execute fallback logic, authorizing a decision with an incomplete evaluation from the three modules. This means transactions were approved or declined with inadequate assessment. Before investing millions to overhaul the authorization platform, however, the organization needed to understand more precisely how these incomplete authorization decisions negatively impacted the bank and its customers.

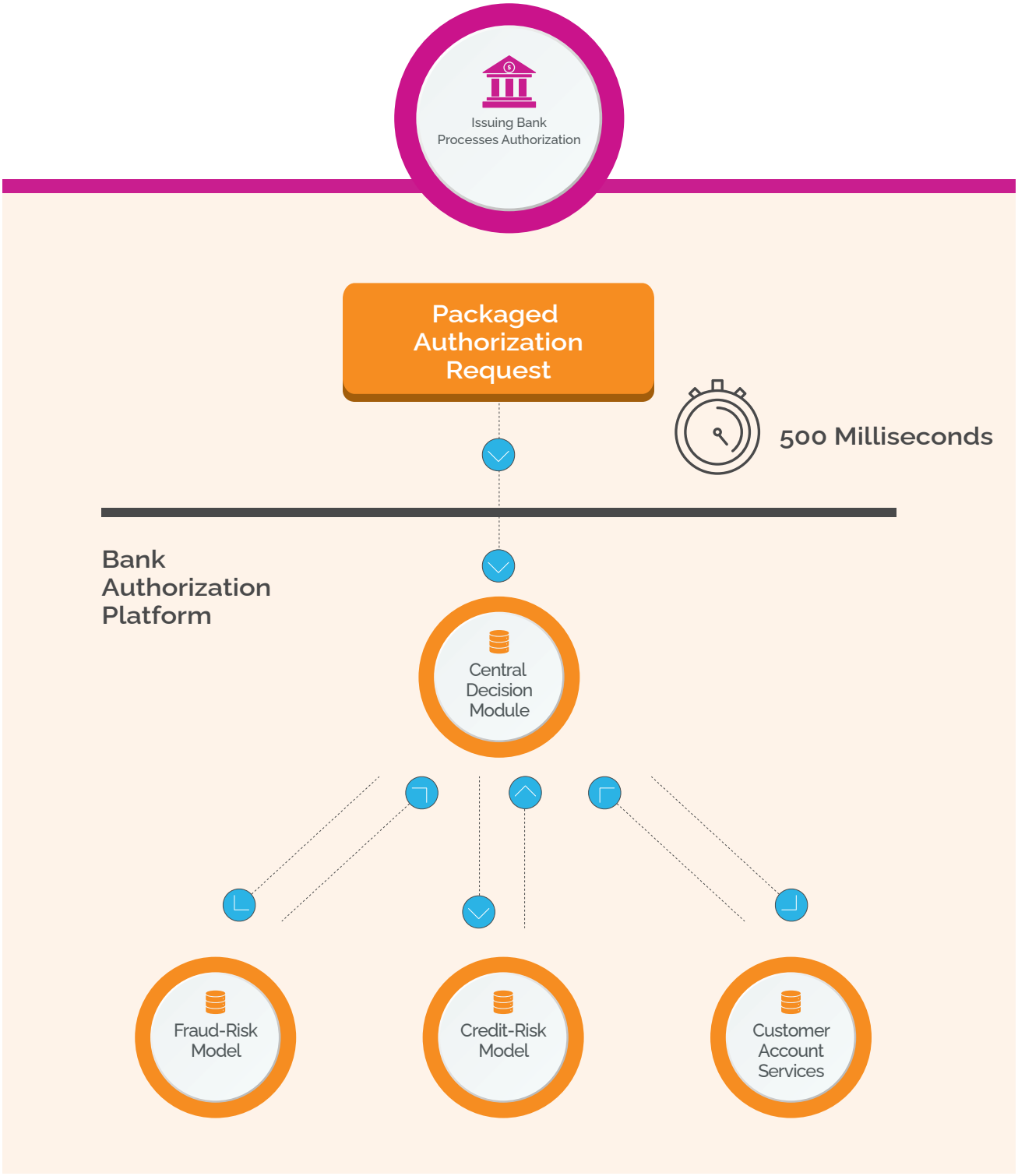

Figure 2:Bank Internal Authorization Process

CHALLENGE

Analyze the impact of making authorization decisions with incomplete information on the bank's financial soundness, regulatory compliance, and customer experience and determine whether an additional investment in technology is the most effective solution for protecting customers and bank assets.

> *"Our toolkit provided insights that drastically changed how the credit card tech team approached module timeouts."*

OUR APPROACH

We began our investigation by determining how many authorization decisions the bank made under deteriorated conditions over the past year. To itemize those decisions, we assessed application log data from the bank's platform, as well as historical authorization data. In addition to quantifying risk by looking at the number of decisions made with incomplete information, we also examined the operation of the central decision model. This assessment enabled us to determine the cause and relative impact of timeouts for each module – fraud risk, credit risk, customer preference – and their impact on each other. Leveraging statistical tests of significance revealed the correlation between the behavior of one module on another.

Our root cause analysis identified timeout patterns in each of the three modules. It also uncovered system limitations. Examining those enabled us to forecast issues that compromised the decisioning platform. Provided with that insight, the bank could then take pre-emptive action to reduce the impact of module timeouts on future transactions.

With some insight on timeout authorizations in hand, we then identified practical scenarios where failure to receive a response from a module could result in an undesirable outcome for the bank or its customers – a risky transaction, for instance, or poor customer experience. After studying the code and documentation for the platform's central decision module, we noted that timeouts created a risky situation only under specific circumstances. The reason for this is because rules governing the final decision are executed in order by priority. For example, if a decline by the fraud-risk module takes absolute precedence over all other rules in the hierarchy, then timeouts from the credit risk and customer preference modules cannot possibly change the decision to an approval. On the other hand, where an otherwise acceptable over-credit-limit transaction is attempted by a low-risk customer, the credit-risk module failing to respond back in time with an approval would result in a decline from the bank. That decision would harm the customer experience and forfeit a revenue-generating transaction for the bank.

Rather than conducting a one-time risk evaluation, we developed a repeatable process and toolkit the bank could use continuously to evaluate all risk scenarios and their respective costs given the volume of timeouts and the logic used to authorize decisions. Since the rules dictating final decisions could change over time, we developed an algorithm that automatically identified risk scenarios for future versions of decision rules. Next, through our partnership with the teams

MEASURABLE RESULTS

- **Provided the bank with a roadmap to save between $500K and $1M in fraud costs and credit-risk approvals** by rebuilding the back-up decision logic found within the third-party processor
- **Re-allocated a $1.2M budget to address resiliency problem**s that have the greatest impact on credit card authorization decisions and costs
- **Developed a continuous risk-monitoring toolkit** that could be incorporated into monthly business monitoring or used to measure the cost of events with severe and prolonged platform degradation
- **Calculated the per-timeout cost for each module and scenario** to help teams understand the relative impact from each module under degraded conditions
- **Produced insights on timeout patterns**, which executive leadership can use to develop a plan for proactively monitoring the authorization platform

specializing in fraud, credit, and customer preferences, we aggregated the cost of timeouts caused by decision modules and then presented this information in the form of dashboards to the bank's leadership.

The outcome of our investigation was unexpected. Our toolkit provided insights that drastically changed how the credit card tech team approached module timeouts. We found that timeouts by the fraud-risk module posed the greatest financial risk to the business, while the customer preference timeouts posed notable regulatory risk in certain countries. Ultimately, we estimated that module timeouts had cost the bank about $130K annually across fraud and credit risk scenarios, which was far less than the $1.2M budget set aside to upgrade the bank's authorization platform.

The more serious, costly problem presented itself in the relationship between the third-party processor and the bank. By quantifying the disruptions between the third-party processor and the bank's authorization platform, we discovered that this stage of the decision process accounted for a larger volume of incomplete authorizations, outnumbering the platform's internal module timeouts by a 15-to-1 ratio. To help the bank make real-world improvements to resiliency and customer experience, we proposed that leadership revamp the back-up decision logic housed within the third-party processor. This solution would allow the bank to reallocate the $1.2M it planned to invest in bolstering the structure of its platform. The empirically grounded roadmap we recommended targeted the highest risk, most impactful types of platform timeouts. It also made more efficient use of limited resources to implement changes that meaningfully improved authorization decisioning for the bank and its customers.