Crowe Horwath

February 2015

Using Model Calibration and Optimization to Reduce Fraud Risk

How Financial Institutions Can Identify Fraud More Effectively While Reducing Costs

By Gregg S. Henzel, CAMS, Troy M. La Huis, CAMS, and Thomas M. Paar, CFE

Audit | Tax | Advisory | Risk | Performance

Bank fraud in essential payment services – debit and credit cards, wire transfers, automated clearing house (ACH), checks, and deposits – is on the rise. The perpetrators prey on weak internal controls at relatively vulnerable institutions. The proliferation of online and mobile banking activities only heightens the fraud threat. To reduce the risk of being the next news story about a breach, banks and other financial institutions must work to increase in-line fraudulent transaction detection rates. At the same time, banks can lower the cost of identifying fraud by reducing false-positive findings. A five-step program of anti-fraud model calibration and optimization enables an institution to continually assess and enhance its fraud prevention effort.

Uncovering Fraud: Many Organizations Do a Poor Job

In November, Crowe Horwath conducted a webinar titled "Fraud Data Analytics," which delved into the challenges of fraud data analytics and the use of prevention and detection rules. The attendees came from several industries, but most were from banks and other financial institutions.

During the webinar, we asked attendees, "What are your current fraud detection rates?" With this question, we sought to determine how effective the attendees' companies are in identifying fraud cases.

About half of those surveyed indicated that they capture less than 75 percent of the fraudulent activity. About 20 percent of their peers responded that they identified and prevented 90 percent or more cases of attempted fraud.

If you were contemplating perpetrating fraud, which of these organizations would you target? Obviously, you would attack where detection rates are low – that is, those organizations that are most vulnerable to fraud.

Fraud Detection Rate	More Than 99%	More Than 90 and Less Than 99%	More Than 75 and Less Than 90%	Equal to or Less Than 75%
Percentage of Respondents	4%	17%	30%	49%

The webinar attendees were then asked, "What are your current false-positive rates?" The aim of this question was to determine how efficiently respondents' companies are performing fraud detection – the lower the rate, the more efficient the performance is.

About 40 percent of respondents reported a false-positive rate higher than 25 to 1. (In other words, for every 25 decision alerts reviewed by an analyst there is one case of fraud.

False-Positives Rate	Less Than or Equal to 5:1	Above 5:1 and Less Than 25:1	Above 25:1 and Less Than 200:1	Above 200:1
Percentage of Respondents	24%	35%	30%	11%

High false-positive rates present two challenges to organizations. The first is cost: As rates rise, fraud prevention requires more labor and becomes more expensive. Indeed, at very high rates, prevention becomes so costly that – from a purely economic view – it could be cheaper simply to let fraud occur.

The second problem with high false-positive results is how it affects the engagement level of those analyzing the company's data for evidence of fraud. When rates start to climb above 25:1, analysts know their next alert is unlikely to reveal fraud. Their incentive to remain diligent declines; their minds wander, and morale erodes. In contrast, when false-positives run 5:1, analysts know that they are just moments away from potentially uncovering another instance of fraud. They're engaged, focused, and efficient.

The ultimate goal is to capture and harvest good alerts while minimizing the occurrence of false-positives. Only 47 of the 288 respondents (16 percent) followed the practice of having 90-percent-plus detection rates and false-positive rates below 25:1. And only eight (3 percent) were in an elite group, with both 99-percent-plus detection and false-positives at or below 5:1.

To gain a sense of how well an organization's anti-fraud effort is performing, the organization can, and should, compare its results against the results of its peers. Ultimately, however, each company defines its own anti-fraud goals and how to achieve them.

Managing Fraud Risk With Model Calibration and Optimization

Three years ago, a well-known national financial institution had annual fraud losses of more than $10 million, and its false-positive alert rate averaged more than 200:1.

Today its losses are down 95 percent. The improvement came largely from more timely detection – in other words, identifying the fraud during the flow of the transaction and before the release of monies from the institution's control. At the same time, the bank reduced its false-positive rate to below 5:1. What makes this decline, along with the drop in fraud losses, particularly impressive is that the bank's business grew more than 20 percent during the same three-year period.

These results were achieved through enhanced anti-fraud model calibration, an effort to assess, monitor, and improve the bank's fraud protection program. Calibration requires the bank to:

1. Develop a calibration and monitoring approach that includes procedures for calibration, prioritization, rule implementation and justification, and a go-live strategy.
2. Plan and execute rounds of preproduction calibration for selected models and rules to optimize effectiveness and yield before promotion to production and optimization.

Fraud model calibration is a five-step, continuous cycle.

Building a Strong Fraud Data Analytics Program

1. Start small; introduce analytics in manageable bites.
2. Concentrate on the data that exists, not what you wish existed.
3. Present information in ways that recognize the role and needs of individual users. Some need detail; others just want the message.
4. Support a data governance program that comprises data management, quality, security, strategy, and architecture. Strong data governance is a prerequisite of strong data analytics.
5. Don't try to do everything – just do what's right for your organization.

1. Identify Model Requirements

A documented coverage assessment is the first step a financial institution must take. Depending on the size of the exposures, banks and other financial institutions will decide to emphasize different areas. The documented coverage assessment is a process that identifies where fraud may occur in the bank and where the bank's energies should be focused – what it will monitor and based on what requirements.

As discussed in the Crowe article "Fraud Decisions : Get a Competitive Edge by Making Sound Decisions Quickly," time is of the essence. A fraud scheme is already underway before the bank processes the transaction; the bank's opportunity to thwart the fraud is before it makes final payment on the transaction. For fraud monitoring, banks have to determine the best time frame, which will differ by product or function.

For example, wire transfers need to be monitored in real time, as do credit cards. On the other hand, while real-time monitoring for ACH may be preferable, a four-hour delay may be satisfactory. The acid test for determining the monitoring time frame is when final payment occurs. For example, with wire transfers, it's immediate and irrevocable; with ACH, there's a delay.

Gaps and inefficiencies need to be assessed at this stage as well. Banks must look at the incremental pieces of data that will help them improve their detection and false-positive rates. An example: An institution should match the customer's Internet protocol (IP) address to the location of the customer for that transaction. If the IP address is in the Middle East, and the transaction takes place in Chicago, that transaction might be more risky.

To summarize this phase of the program:

- Through a documented coverage assessment, the bank identifies all areas of risk and the mitigating transaction monitoring reports and rules in place. The process helps identify potential monitoring gaps while providing the baseline justification for the transaction monitoring program.
- The bank analyzes actual losses owing to fraud to determine if a control failed or was absent altogether.

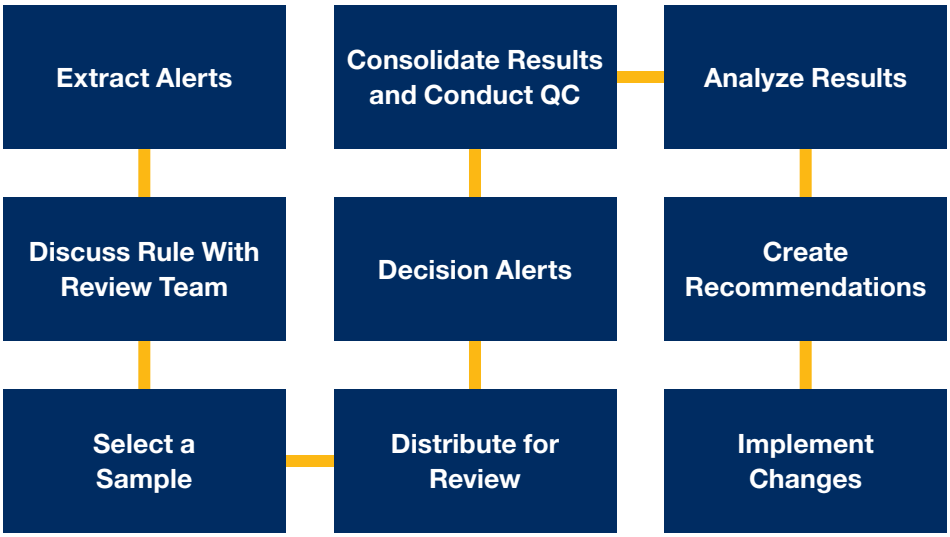
2. Prioritize Gaps and Inefficiencies

Once monitoring requirements, gaps, and inefficiencies have been identified, the bank prioritizes the calibration opportunities, based on risk factors such as products offered, branch locations, past losses, and current trends as well as the institution's level of risk tolerance.

3. Perform Analysis and Calibration

Calibration includes changing the rules or logic for the existing data sets, as well as adding data that can improve the detection of false-positive alerts. An example: Adding device identification data to determine whether the device previously has been used by the customer, who is likely to use the same device for every transaction. The exhibit shows the typical steps in the calibration process .

Exhibit: Typical Steps for Model Calibration



Source: Crowe analysis

Calibration must be done continually, because perpetrators are constantly refining their skills and adjusting their strategies as they learn what the bank is doing. Always seeking to exploit a vulnerability, they work to know where the controls are, and they pounce on inefficient mechanisms.

The following points are essential to this phase:

- An analytical approach is adopted to review alert quality in each report or rule used for monitoring.
- The analysis helps to assess threshold and parameter enhancement opportunities.
- Calibration is applicable to both real-time alerts or reports and point-in-time reports, which usually reflect the prior business day.

4. Implement Monitoring Requirements

The key to implementing monitoring requirements successfully is performing tests in the production environment with real data to confirm that processes are working as expected.

Two points should be emphasized:

- Any potential changes to the transaction monitoring program must include a regimented, documented control process. This process helps to ensure that appropriate approvals are obtained and justifying documentation is maintained for all system changes.
- Proposed rule changes should include an analysis of the potential increase or decrease in the expected dollar risk.

5. Ongoing Assessment and Optimization

Assessment and optimization entail:

- Developing appropriate ongoing assessment metrics to enhance monitoring opportunities, which effectively address changes to the bank's risk factors and evolving patterns of fraud
- Instituting a rule review matrix that helps to ensure that every rule is reviewed at least yearly

Importantly, continuing assessment and optimization requires that an independent group, either internal or external, validates the models used for detection. Financial institutions are well accustomed to using models in their operations and must independently test their assumptions about risk in the anti-fraud model.

Large Benefits From Model Calibration

Fraud risks pose an increasing threat to bank operations and profitability. Too often, however, the anti-fraud programs of financial institutions are too costly and not effective enough. Given adequate resources and the focused attention of management, a continuous program of anti-fraud model calibration and optimization can help financial institutions make substantial strides in their anti-fraud efforts.

Contact Information

Gregg Henzel is with Crowe Horwath LLP and can be reached at +1 630 575 4350 or gregg.henzel@crowehorwath.com.

Troy La Huis is a principal with Crowe and can be reached at +1 616 233 5571 or troy.lahuis@crowehorwath.com.

Tom Paar is with Crowe and can be reached at +1 630 575 4324 or thomas.paar@crowehorwath.com.

www.crowehorwath.com