How the Past Changes the Future of Fraud

Addressing payment card fraud with models that evaluate multiple risk dimensions through intelligence

Card fraud costs the U.S. card payments industry an estimated USD 8.6 billion per year. Although just 0.4% of the USD 2.1 trillion in U.S. card volume per year, this number remains a troubling area for the industry due to the volatile nature of fraud.

– Aite Group, January 2010

Fighting fraud continues to rank high among strategic business drivers in retail banking. Over the last few years, the payment industry has adopted technologies that significantly reduce fraud rates in some areas. But just when banks think they’ve got a handle on the latest fraud tricks, new ones emerge, attacking across regional boundaries, channels, and from every angle imaginable.

One way to tackle payment card fraud is implementing a holistic, multi-pronged strategy based on knowledge discovery at every stage of the card life-cycle. By moving away from an existing one-size-fits-all model and applying a custom or network model that is based on detailed views of global transactions, companies can cost-effectively reduce risk and prevent losses.

Banks have another option beyond the current models and authorization controls. They can create better authorization strategies at the point of sale and lower customer disruption rates by implementing more operational efficiencies in the back office. This will help with retention of their most profitable customers and portfolios.

This paper discusses the science that MasterCard applies to its network and custom fraud detection models and how these two approaches are bringing more intelligence and incremental value to legacy systems today.

### DISTRIBUTION OF ISSUER FRAUD LOSSES BY TYPE: 2008-2009

<table>
<thead>
<tr>
<th>Type</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNP</td>
<td>32.60%</td>
<td>38.20%</td>
</tr>
<tr>
<td>Counterfeit</td>
<td>36.80%</td>
<td>37.40%</td>
</tr>
<tr>
<td>Lost/Stolen</td>
<td>20.60%</td>
<td>18.10%</td>
</tr>
<tr>
<td>Misc Fraud</td>
<td>10.00%</td>
<td>6.30%</td>
</tr>
</tbody>
</table>
The role of authorization is vital in preventing fraud. This means the network is the issuers’ front-line of defense and must provide input into their fraud scoring and decisioning systems quickly. It must also support continual evaluation of issuer fraud performance against industry standards.

Expert Monitoring Solutions, MasterCard’s comprehensive fraud management suite, addresses fraud by using specific models to evaluate multiple risk dimensions for issuers — allowing them to make authorization decisions based on their own risk tolerance. It is a data-driven approach that builds insights into a wide variety of fraud models tailored to the unique fraud exposure of diverse issuer portfolios. The three components of Expert Monitoring Solutions are designed to flexibly accommodate global market needs:

- **Fraud modeling platform** — a world-class data mart used by the modeling team to assess customer needs and identify fraud pain points. It delivers both standard network models and customized issuer models to better address the customer portfolio.

- **Scoring platform** — delivers model-generated scores within milliseconds in a real-time authorization message, or in a neartime authorization advice message delivered just after the issuer approval decision. The fraud scores are used automatically by the issuer authorization system in real-time as an input to approve, deny, or refer the authorization. They also serve as input to fraud investigation teams when making the decision to monitor or investigate a potential case of fraud.

- **Case management and reporting tools** — an optional part of the package offering both hosted and local tools to enable fraud management personnel to quickly and easily manage cases.

This strategy allows customers to gain that extra bit of insight that can make the critical difference between catching the fraud on the first or second transaction versus the sixth or seventh transaction.

---

**Data Mart Defined**

MasterCard uses a dedicated, fit-for-purpose data mart to collect the essential data needed to identify global fraud trends. In contrast to a data warehouse — which is an enterprise-wide data storage repository — MasterCard’s fraud data mart is constructed with one objective: to aggregate the data, tools and knowledge needed to optimize fraud detection. The result is a world-class facility for data mining and analysis, allowing the past to help predict the future trajectory of fraud.
To help issuers reduce losses efficiently, MasterCard enhanced its global network to allow more intelligent scoring of transactions. By using a fraud score in the authorization request in real-time, issuers can enhance their fraud detection capabilities and operations. They can prioritize transactions for review and utilize scores as a highly reliable factor in existing fraud detection systems.

**Expert Monitoring provides artificial intelligence scoring that:**

- Uses data history to create a fraud model that is deployed against current transaction activity to highlight suspicious transactions compared to model data
- Supplements issuer scoring processes reliably
- Ensures fraud models are timely and current for optimal fraud detection — enabling customers to frequently fine-tune the performance of their fraud model by adjusting rules and parameters

MasterCard is currently building feedback loops into the process to ensure that it can monitor model performance over time, and proactively work to refresh the fraud model as fraud patterns change.
Expert Monitoring scores are driven by artificial intelligence and typically evaluate over 100 variables in determining the transaction risk level. The MasterCard Worldwide Network delivers more insight and tools to predict and detect fraud, with a particular focus on global and country-specific insights as fraud transcends borders. All this helps issuers make smart decisions at the point of sale.

MasterCard integrates a variety of data mining and neural network tools with payments expertise and data analytics to train its fraud models on the attributes of recent fraud activity. The result is a set of models that can effectively anticipate future fraud scenarios. Based on data mining using a world-class data mart that aggregates the extensive assets of the MasterCard Worldwide Network, these models include:

- Global authorization data leveraged across MasterCard’s integrated network and carefully captured, stored and cleansed
- Issuer-reported fraud data which provides a high degree of granularity at the transaction level
- Supplemental data from internal and external data sources, including insights from investigation of account data compromise events
- Market-leading data mining tools to allow modelers to quickly leverage the fraud data mart and build targeted models

By unlocking the global intelligence in the network, MasterCard experts can build fraud models which are tailored to identify the latest fraud patterns across geographical markets, transaction types, card products, and cardholder segments. Models are carefully segmented to ensure that they can uniquely capture both local and regional fraud trends and processing patterns.

For example, peak spending seasons vary by country. Data has shown that in Europe card usage may peak in the summer, while in the U.S. the peak season is centered around the months of November and December. Models are tuned to expect higher transaction volume during the typical peak season period for the country or region, which helps control false positive rates.

Other important differences among fraud patterns can be found in card products. For instance, international fraud on U.S. corporate cards is higher than on a U.S. consumer credit portfolio as measured in basis points. By accounting for this difference, false positives for the U.S. Consumer Credit model can be reduced, and cross-border fraud on commercial cards can be identified accordingly.

Data analysis shows that fraud strategies must be refined by portfolio or customer segment. The same approach that is used with affluent customers, for example, may not work for non-affluent consumers. MasterCard fraud models are flexible and capable of adapting to these differences.
With the ability to leverage a global data mart, MasterCard provides an extensive variety of finely-tuned network and custom fraud models segmented by a wide variety of criteria for significantly higher fraud detection over industry-standard consortium models. MasterCard develops fraud models that directly address specific pain points by drilling into and differentiating legitimate activity versus fraudulent activity.

**Network models** are primarily targeted to address generalized fraud trends across market areas or products. These models are developed from MasterCard data using multiple data points and are applicable to common customer portfolio segments. They are different from consortium models which are often based on input from a limited number of financial institutions, which can skew the data used to train the model. The network models built by MasterCard utilize all the data that traverses the MasterCard network, so they are more robust and can identify normal and customary transactional patterns from suspicious or out-of-pattern behavior.

**Custom models** are developed from customer-specific data points as well as MasterCard data. MasterCard enables issuers to customize fraud models to the unique needs of their proprietary portfolios for greater precision in fraud detection.

Within the category of custom models, MasterCard uses two development methods to align the model to an issuer’s fraud strategy. In the first approach, a completely dedicated model is built for a specific issuer portfolio or set of portfolios.

In the second approach, a modified network model is created using two-stage modeling techniques to optimize an existing network model and address a specific issuer fraud strategy. This type of model can suppress or amplify scoring in specific areas and is designed to align scores to the business objectives and the queue prioritization strategy of the fraud back office.

Though targeted modeling can be challenging, it is an important approach which brings longevity to solutions for issuers around the globe. Interaction with multiple customers underscores the need for this approach, and MasterCard has received positive testimonials from its users of these two types of models.
CASE STUDY

Conversion from network model to custom model

The challenge: An issuer with a premium consumer airline portfolio was experiencing high false positives due to the high level of online purchases and cross-border travel, when compared to typical consumer credit behavior in the market. At the same time, overall transaction volume was increasing due to a portfolio conversion that significantly raised the number of accounts the fraud team was responsible for monitoring. Given constraints in staffing for fraud investigation, the volume of alerts was unmanageable.

MasterCard’s response: MasterCard worked with the issuer to transition from a network fraud model to a custom model which aligned to the needs of this unique portfolio. The new model was delivered on time within a target five-month project plan, and resulted in a low false positive ratio and high rate of detection.

The results:

“We are seeing far fewer false alerts, so we’re not getting overwhelmed by the high volume of alerts any more, which makes our work far easier than it used to be. The false positive ratio was reduced significantly on the very day the new model was implemented … The new custom model is now in its third week of production and we are more than happy with the performance of the model.”

– Bank Fraud Executive
**CASE STUDY**

**Canada network model**

**The challenge:** The Canada market had experienced a spike in fraud that resulted in a significant one-time increase in fraud basis points. The unique signature of this event was not likely to occur again in the near term, but the Canada model needed to be trained to recognize the leading indicators of this type of fraud spike.

**MasterCard’s response:** Through corrective sampling techniques, MasterCard tuned the Canada model to focus primarily on business-as-usual fraud. Close analysis and data mining of the attributes of the fraud attack led to the identification of fraud rules that were integrated into the Canada model. A series of blind tests were conducted to test the behavior of the model during the fraud spike and determine the level of fraud detection that would have been achieved if the model had been in production during the fraud attack.

**The results:** At an account false positive of 20:1, the Canada model successfully scored both BAU and unique fraud attack scenarios, with the blind test scores during peak fraud events actually exceeding expected results for the model.

**CANADA CREDIT MODEL PERFORMANCE**

This chart compares Transaction Detection Rates (TDR), Account Detection Rates (ADR), and Value Detection Rates (VDR) for the overall Canada Credit Model vs. two months of blind test traffic processed by the model.
With Expert Monitoring, MasterCard is opening up more choice and more options for issuers. Strong results from customer trials exceed current industry benchmarks for detection rates and false positives.

**Other benefits for issuers include:**

- Improved accuracy in fraud detection rates with precise fraud models tuned to the unique needs of issuers portfolios, which enable a fraud score proven to deliver significant, double-digit lift in fraud detection rates.

- Lower false positive rates and improvement of cardholder service with sophisticated transaction monitoring services. Expert Monitoring evaluates transactions at the point of sale to deliver a fraud score that can dramatically improve the predictive capability of your scoring solution — lessening the inconvenience to customers caused by investigating transactions that appear fraudulent but prove to be legitimate.

- Reduction in IT investment in fraud with a turn-key, configurable and globally integrated solution that hosts scalable transaction monitoring and scoring capabilities that can be implemented according to specific needs — without significant capital investment in new technologies, development resources, and time to market.

Securing the payment processing environment is a top priority. By leveraging the ongoing investment by MasterCard in state-of-the-art fraud detection systems, network monitoring technologies, and security expertise, issuers can predict and prevent fraud more accurately and comprehensively, and improve collection and recovery of fraud-related losses.

*For more information, please contact MasterCard at risksolutions@mastercard.com or your MasterCard account representative.*