Fraud Analytics in Retail Banking
Conquering the Challenges Posed By IT, And Talent, to Operationalize Fraud Analytics, to Stay Ahead Of Fraudsters

Anupam Jain, Practice Director

Issuers, merchants, and acquirers of credit, debit, and prepaid general purpose and private label payment cards worldwide experienced gross fraud losses of US$11.27 billion in 2012, up 14.6% over the previous year. Fraud losses on all general purpose and private label, signature and PIN payment cards reached US$5.33 billion in United States in the same period, up 14.5%. These are truly big numbers, and present the single-biggest challenge to the trust reposed in banks by customers.

Besides the risk of losing customers, direct financial impact for banks is also a significant factor. Upon reporting of a fraudulent transaction by a customer, the bank is liable for the transaction cost, it has to refund merchant chargeback fee, as well as additional fee. Fraud also invites fines from regulatory authorities. The recently-passed Durbin Amendment caps processing fee that can be charged per transaction, and this increases the damage caused by unexpected fraud losses.

The rapidly rising use of electronic payment modes has also increased the need for effective, efficient, and real-time methods to detect, deter, and prevent fraud (see Figure below).

Business drivers to detect and prevent fraud

Risk of losing customers
- Fraud erodes the trust in banks
- Leads to lower C-SAT, higher churn, and harder customer acquisition

Financial losses
- Banks liable for transaction costs, merchant chargebacks, and additional fees
- Regulatory changes (such as Durbin Amendment) have increased the financial impact of fraud

Increasing incidence of fraud
- Rising use of electronic payments and technology advancements are increasing the incidence of fraud
- Requires complex and large scale monitoring of people, places, systems, and events

Benefits
- A top 5 U.S.-based large global bank reduced fraud loss by ~40% (US$2 million savings)
- HSBC (U.S.) increased transaction monitoring from 25% to 100%
- A large U.S. bank reduced false alarms by 40%
- A community bank reduced time to review alerts from four hours to less than 30 minutes

Keys to operationalize fraud analytics in retail banking
- Continuous updating and refining of models
- Designing self-learning algorithms
- Global knowledge sharing
- Pooling resources to fight fraud

Fast reference
Why important.........................1
Impacts of analytics....................2
Operationalizing analytics.............3
Conclusion.............................4

How analytics is helping in fighting fraud?

Fraud in retail banking is an umbrella term describing unlawful mechanisms with the aim of either securing unauthorized funds or goods/services without payment. It can be broadly classified into:

- Card fraud – Identity theft, phishing, mail and phone fraud, and online fraud
- Deposit fraud – Fraud against bank deposits, check fraud, online banking fraud, mobile banking fraud, and wire fraud

Most of these frauds are low-value and high-volume in nature. So they present an excellent opportunity for analytics to identify patterns and recommend preventive action. Many of the techniques employed to detect frauds require recognizing identical/repeating pattern matches of people, places, systems, and events. There are various methodologies employed for fraud detection, enabling a wide range of solutions (see Figure below). Beyond statistical techniques, artificial intelligence is also starting to be leveraged to prevent fraud.

Effective use of analytics to fight fraud can help improve profitability in the cards business (this has acquired even greater significance after the passage of Durbin Amendment), reduce payouts and legal hassles, and most importantly, improve customer satisfaction. Time taken to act, once fraud is detected, is also critical and often a last step human intervention is required to act on fraud alerts. Analytics help improves the ability of existing fraud experts to focus on real threats more efficiently and effectively (by expanding transactions monitored and reducing false alerts). Automated alerts can also be sent to the customer directly. However, the biggest value that analytics brings to the table is to go beyond detection – by predicting and even preventing fraud. Advanced analytics help in recognizing patterns of fraudulent transactions, and then use these to be one-step ahead of fraudsters, predict the next such fraud in progress, and recommend taking preventive action, saving both the bank and the customer.
Successfully operationalizing fraud analytics in retail banking

Initiatives to develop predictive and prescriptive analytics based on pattern recognitions, typically hit the following major operational challenges:

1. **Balancing priorities (competitive offering, customer convenience, and security):** The triad of competitive offering, customer demands, and security pull in different directions – competitive forces strain banks’ abilities to do more of fraud prevention, customers want cards to be accepted widely, security demands restricted, and careful usage. Banks have to walk the tightrope between the three forces to succeed

2. **Resource constraints (both IT and talent):** Multiple algorithms and engines’ results need to be integrated and interpreted for predicting fraudulent activities, presenting a significant computing challenge. The filtering out of false alarms generated by algorithm(s) adds to the complexity in the process

3. **Staying ahead of fraudsters:** Fraud analytics models need constant adjustment and enhancement. Once a fraud technique is identified, the model quickly needs to assimilate that information, and start looking for the next loophole, that a potential fraudster may exploit. Since the entire game hinges on being able to prevent commitment of fraud, the pressure is always on the banks to be ahead of fraudsters

Emerging best practices to successfully operationalize fraud analytics:

- **Continuously update and refine models:** Banks are increasingly relying on external data (outside of banks’ systems) to predict frauds, based on trends impacting their peers, and the broader industry. While on one hand, the models need to be kept updated with the latest external data, on the other, they also need to be continuously improved in order to keep accepting newer kinds of data. These helps the models removes barriers to their useful life

- **Design self-learning algorithms:** Models than can learn from the positive identifications that they make, and, hence, evolve and strengthen their functioning reduces false alerts and help banks stay ahead of fraudsters. Also, enabling sharing of results between algorithms helps in triangulation of results

- **Global knowledge sharing:** Business units within banks are today collaborating more between themselves, and making sure that lessons learnt in one geography for fraud prevention are utilized in other geographies

- **Pooling resources to fight fraud:** Banks are starting to realize the power of working together to fight fraud more effectively. Building individual models is costly and time-consuming. The solution is for banks to move to network-based models, where fraud detection algorithms from different banks work together for the group, and help achieve more extensive and better results, while keeping the costs low as well
Conclusion

Frauds will increase as transaction volumes rise and transactions become more virtual. Rapidly advancing technology is both an ally and an enemy – it opens newer avenues for fraudsters but also provides options for banks to stay ahead. Operationalizing analytics built on advanced models, self-learning algorithms, and global knowledge sharing may be an important weapon for banks in this conflict.

This study was funded, in part, by support from Genpact

About Everest Group

Everest Group is an advisor to business leaders on next generation global services with a worldwide reputation for helping Global 1000 firms dramatically improve their performance by optimizing their back- and middle-office business services. With a fact-based approach driving outcomes, Everest Group counsels organizations with complex challenges related to the use and delivery of global services in their pursuits to balance short-term needs with long-term goals. Through its practical consulting, original research and industry resource services, Everest Group helps clients maximize value from delivery strategies, talent and sourcing models, technologies and management approaches. Established in 1991, Everest Group serves users of global services, providers of services, country organizations, and private equity firms, in six continents across all industry categories. For more information, please visit www.everestgrp.com and research.everestgrp.com.