Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Cards | the way we see it

# Credit Card Transaction Fraud and Mitigation Trends

## Latest credit card fraud trends and mitigation methodologies

People matter, results count.

# Contents

# 1 Highlights

Despite the credit card industry's effort to fight fraud, losses are increasing globally. In 2009, overall card fraud losses increased by 12.8% to reach €4.9 billion, and total credit card fraud losses reached approximately €2.4 billion, up from €2.1 billion in 2008. Card fraud continues to increase as fraudsters find more ways to hack into processors' data centers and merchants' databases.

The growing level of losses is driving an increase in the industry's cost to fight fraud, resulting in a negative impact on profitability. According to a recent study, in 2010 U.S. financial services institutions suffered an estimated US$2 to US$8 billion in fraud losses associated with unauthorized transactions. Total merchant fraud losses, which include interest or fees paid by merchants to financial institutions and the cost of replacing or redistributing merchandise to consumers in addition to the actual fraud amount, reached a US$102.3 billion or €76.7 billion.[1]

This paper discusses global credit card fraud with a special focus on the implications for financial services institutions, merchants, and consumers. To fight credit card fraud globally, financial firms are increasingly centralizing their fraud management systems to maximize the bottom line by lowering the volume of fraudulent transactions. They are also moving from in-house solutions to commercial enterprise fraud management (EFM) products. Finally, in the area of web fraud detection (WFD), advanced end users are increasingly seeking self-learning predictive models—mathematical models based on artificial intelligence—that can run in parallel to the rule-based models.

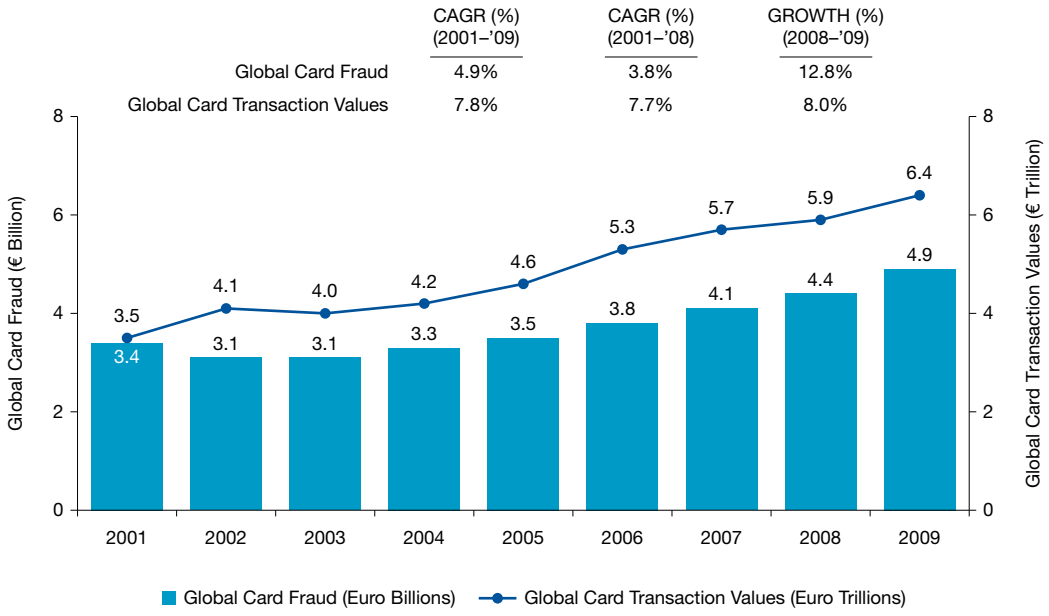
[1] True Cost of Fraud study, LexisNexis, 2011

# 2 The Rise of Credit Card Transaction Fraud

## 2.1. The Growth and Cost of Credit Card Fraud

Overall card fraud numbers have increased substantially in 2008 and 2009 with annual growth rates of 7.2% and 12.8% respectively[2]. Global card fraud losses reached €4.9 billion in 2009, despite the industry's effort to fight fraud, while credit card fraud was estimated to have increased between 11.5% and 14.1% to reach €2.4 billion in 2009, up from €2.1 billion in 2008. Card fraud continues to increase as fraudsters come up with innovative hacking techniques that provide access to more consumer accounts than stolen cards and identity theft. The growing level of losses is driving an increase in the cost to fight fraud, and at the current growth rates, card fraud is estimated to grow to $10 billion annually by 2015[3].

**Exhibit 1: Global Card Fraud (€ Billion) and Global Card Transaction Values (€ Trillion), 2001–2009**



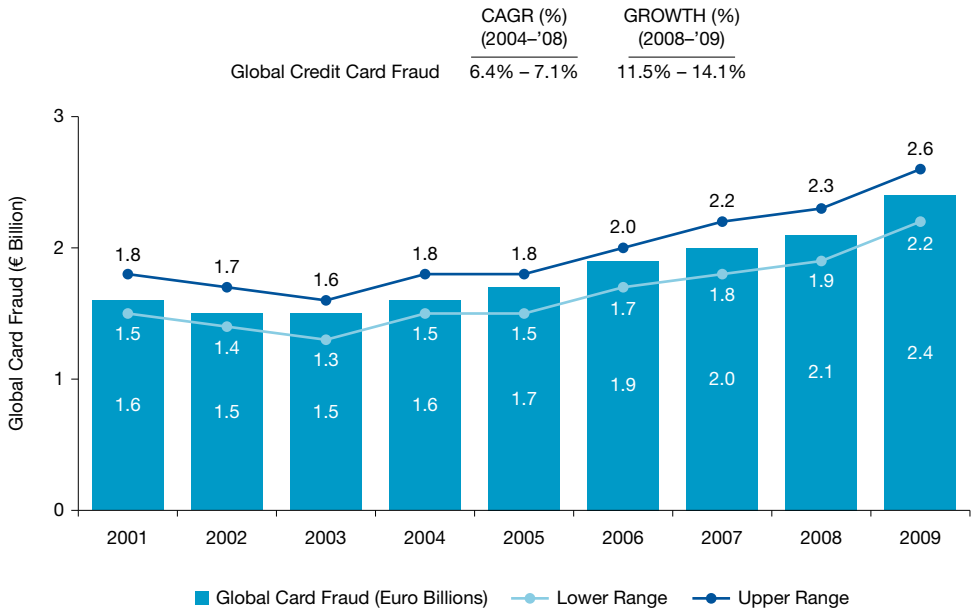

Source: *World Payments Report 2011*, Capgemini and Capgemini Analysis

[2] *World Payments Report 2011*, Capgemini Analysis

[3] Global Card Fraud, The Nilson Report, June 2010

Despite the wider implementation of the Payment Card Industry Data Security Standard[4] (PCI DSS) among large merchants, the number of customer accounts stolen still remains high. In the U.K., where the EMV[5] (Europay, MasterCard® and VISA®) standard is being implemented, some evidence suggests that the card fraud loss rate declined. The exact contribution of the EMV standard to the decline is difficult to determine and the cost of EMV migration in many markets outweighs the cost of the fraud it may prevent.

**Exhibit 2: Global Credit Card Fraud (€ Billion), 2001–2009**




Source: Capgemini Analysis, 2011; *World Payments Report 2011*, Capgemini; Credit card statistics, industry facts, debt statistics from www.creditcards.com.

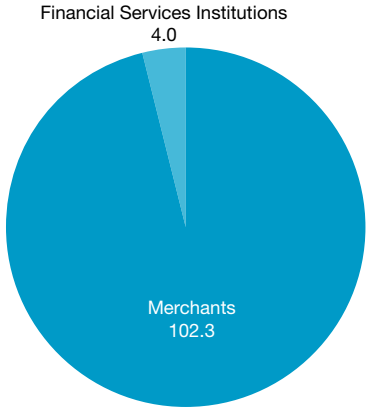
In any given fraudulent transaction, the financial services institution, the merchant, and the consumer are the primary casualties. In 2010, financial services institutions in the U.S. are estimated to have lost between US$2 and 8 billion in fraud associated with unauthorized transactions. In addition to these actual write-offs, firms also spend heavily on operational costs associated with resolving fraud and on legal and punitive costs imposed by regulators and governments. Governments can even take over the control of operations in case of failure on the part of financial services institutions to effectively manage fraud.

[4] PCI DSS is a standard that provides an actionable framework for developing a robust payment card data security process including prevention, detection and appropriate reaction to security incidents and is offered by PCI Security Standards Council, https://www.pcisecuritystandards.org/security_standards/

[5] EMV is a global standard for inter-operation of integrated circuit cards and IC card capable point of sale terminals and automated teller machines, for authenticating credit and debit card transactions

Fraud can cause companies to suffer loss of brand value which impacts their growth plans, leading to erosion in shareholder value. During 2010, merchants in the U.S. lost a total of US$102.3 billion (€76.7 billion) in fraud losses due to unauthorized transactions. This estimate includes interest or fees paid by merchants to financial institutions and costs to replace or redistribute merchandise to consumers in addition to the actual fraud amount[6].

**Exhibit 3: Estimated Cost[7] of Fraud ($ Billion), 2010**




Source: Capgemini Analysis, 2011; True Cost of Fraud study, LexisNexis, 2011

## 2.2. Common Fraud Techniques

With the advent of social networking and technology, fraudsters have found innovative new ways of committing fraud. Several commonly employed techniques are described below.

**Account takeover**

This has traditionally been the most popular non-technology method to commit fraud. Fraudsters manipulate consumer accounts by adding their own information to the victim's account, usually by changing the victim's account email address or physical mailing address.

**Friendly fraud**

Fraud committed by someone who actually knows the fraud victim is steadily rising. The victims in this type of fraud are usually well-known to the perpetrators and can be family members, colleagues, neighbors, friends, or acquaintances, among others. Friendly frauds are usually difficult to detect as perpetrators have a fair idea about the victim's personal information, habits, and movements, and are able to conceal their fraud longer. Also, victims of friendly fraud usually do not report the fraud to authorities as it affects their personal relationships[8].

[6] True Cost of Fraud study, LexisNexis, 2011

[7] Cost for merchants is defined as the total cost incurred by merchants in addition to the actual value of crime and involves interest and fees paid by merchants to financial institutions and the cost for replacing or redistributing merchandise to consumers

[8] 2011 Identity Fraud Survey: Consumer Version, Javelin Strategy & Research, February 2011

**Bust-out fraud**
Recently, bust-out or sleeper fraud has gained prominence and is causing substantial losses to financial services institutions. Bust-out fraud is an intentional fraud committed by those consumers who use all the available credit in a particular credit card or cards (from single or multiple institutions) and then skip the final payment.

In this kind of fraud, the consumer first builds good credit history, applies for a credit card, uses credit and makes regular payments, and finally exhausts all the available credit (bust out) with no intention of paying it back. Bust out fraud is usually committed by those consumers who reside in a particular country on temporary basis such as students or migrant employees and who plan to move to their home or another country with no intention of returning.

**Cloning and malware**
Cloning and malware are the most popular fraud methods that are aided by technology. Cloning card fraud is when criminals use details on the tracks[9] on the magnetic strip of a credit card to create replica payment cards for committing fraud. Malware is malicious software designed to gain unauthorised access to a database or network or operating system or computer without the consent of the user.

Cloning can be elaborated and classified into carding and BIN attack. Carding is a technique in which computer programs (generators) are used to produce a sequence of credit card numbers which are then tested to check for valid accounts. BIN attack is a method in which one good card number is obtained and valid card numbers are then generated by changing the last four numbers.

**Skimming and phishing**
Skimming and phishing are gaining popularity among fraudsters. Skimming[10] is the theft of payment card information using skimming devices while someone is performing legitimate transactions such as purchases at grocery markets or gas stations. Phishing card fraud is when a criminal obtains a consumer's financial or personal information by sending an authentic looking e-mail to them, which in turn lures them to a fake website that looks almost similar to the victim's institution.

[9] The magnetic stripe of a payment card has two tracks (track 1 and track 2) that have recorded card details
[10] 2011 Identity Fraud Survey: Consumer Version, Javelin Strategy & Research, February 2011

# 3 Emerging Fraud Mitigation Trends

As stated earlier, fraud has different implications for different stakeholders. The following sections summarize some of the recent trends witnessed in the fraud industry from the perspective of financial services institutions, merchant/consumer, and technology.

## 3.1. Trends for Financial Services Institutions

Leading industry analysts such as Forrester[11] and Gartner[12] have identified key fraud mitigation trends for financial firms including centralizing fraud management operations, using more real-time external data, migrating from in-house to commercial enterprise fraud management products and upgrading to second generation web fraud detection systems.

**Centralizing fraud management systems helps financial services institutions reduce costs and improve efficiency.**

**Trend #1: Centralize fraud management operations**

Financial services institutions are increasingly centralizing their fraud management systems to combine all the pieces (capabilities, analytics, processes, and oversight) to derive financial benefit by preventing a greater number of fraudulent transactions. To effectively fight fraud, forward-looking financial firms constantly update fraud management systems with new rules, statistical models and acquired knowledge. This process becomes easier and more efficient with centralized systems.

**Trend #2: Use more real time external data**

Several financial services institutions are no longer content with just using regular transactional data to fight fraud. They are also looking at external information obtained from third party vendors and intelligence from social networking sites to improve their capabilities in fraud detection. The addition of this external data to the already existing internal data pool creates larger data sample sizes, thereby improving the accuracy in fraud detection.

**In-house solutions are inadequate in addressing new threats and are difficult to maintain and upgrade due to their architectural complexity.**

**Trend #3: Migrate from in-house to commercial enterprise fraud management (EFM) products**

In a changing business and IT landscape, financial services institutions are increasingly shifting towards commercial EFM products as in-house solutions are inadequate in addressing the latest challenges. For financial services institutions with large transaction volumes, in-house solutions are often inadequate in responding to fraud threats in real-time where as commercial EFM products have the capability process large transactional volumes and also sort and risk-score transactions at a fast rate.

**Trend #4: Upgrade to second generation web fraud detection systems**

High-risk organizations that process huge volumes of transactions are upgrading to second-generation web fraud detection (WFD) systems to counter the increasingly sophisticated and unpredictable attacks. Organizations with sensitive customer data and high risk applications are looking to upgrade to second-generation WFD systems to counter the latest threats such as man-in-the-browser attacks[13].

[11] Enterprise Fraud Management Predictions: 2011 and Beyond, Forrester, December 2010

[12] Magic Quadrant for Web Fraud Detection, Gartner, January 2010

[13] **Man-in-the-Browser** is a Trojan virus that infects a web browser and has the ability to modify pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application

## 3.2. Trends for Merchants and Consumers

The annual *True Cost of Fraud* study from Lexis-Nexis[14] looks at fraud trends among merchants and consumers such as increased identity fraud faced by merchants, increased mobile payments accepted by merchants, and lower fraud costs for consumers in network-branded credit card fraud.

**When compared to regular merchants, online merchants face a higher risk of higher identity fraud.**

**Trend #1: Identity fraud is increasing for merchants**
In the July 2011 survey, losses incurred by merchants due to identity fraud increased to 14% as a percentage of total fraud losses versus 11% in 2010. This trend points to a greater need for improving transaction verification and authentication processes.

Merchants providing an online channel for their businesses faced an even higher increase in identity fraud as it is relatively easier for fraudsters to commit fraud in card not present (CNP) scenarios. Crime is generally rising due to the economic downturn and increased sophistication in criminal fraud methods, and identity fraud is no exception to this rule.

**Trend #2: Mobile payments are becoming more widely accepted by merchants**
In 2011, mobile payments were being accepted by 4% of merchants compared to 1% in 2010. Merchants are increasingly accepting mobile payments with 20% of merchants who currently are not accepting mobile payments indicating they would likely do so in the next year.

Given the increase in smart phone adoption among consumers and willingness of merchants to accept mobile payments, mobile payments are poised for growth. However, merchants must equip themselves with proper fraud mitigation tools to reduce the risk of threats posed by mobile adoption.

**When compared to store-branded card issuers, network-branded card issuers assume greater responsibility in the fraud resolution process, as it is their primary business and has a direct implication on the brand value.**

**Trend #3: Consumers using network-branded credit cards have lower fraud costs**
Average fraud costs for consumers using network-branded cards such as American Express®, Discover®, MasterCard®, and VISA® is less than those using the store-branded cards issued by stores like Wal-Mart or Home Depot. Global networks like American Express, Discover, Master Card, and VISA are enforcing higher security and consumer protection standards on issuers seeking their affiliation.

When compared to store-branded card issuers, network-branded card issuers generally assume greater responsibility in the fraud resolution process, as it is their primary business and has a direct implication on the brand value.

## 3.3. Trends in Technology

Forrester[15] and Gartner[16],[17] have identified new fraud risks due to the increased adoption of mobile devices, web fraud detection shifting from rule-based systems to self-learning predictive models, demand for an enhanced business user interface for alert and policy management, and demand for deployment and support simplicity.

**Organizations will have to adjust their business and IT processes to counter the new fraud risks posed by increasing adoption of mobile devices.**

**Trend #1: New fraud risks due to the increased adoption of mobile devices**
There has been a proliferation of worms with the ability to infect mobile phones, and with the surge in post-PC devices, organizations can longer mandate the use of a specific brand to maintain standards. This leads to increased risk in the form of data theft, rogue applications, and data ownership.

[14] True Cost of Fraud study, LexisNexis, 2011
[15] Enterprise Fraud Management Predictions: 2011 and Beyond, Forrester, December 2010
[16] Magic Quadrant for Web Fraud Detection, Gartner, January 2010
[17] Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities, Gartner, October 2010

Worms have the ability to manipulate the internet connection and can skim transactions that are being executed on a mobile device. They also possess the ability to forward text messages from the victim's mobile device to fraudsters, enabling them to execute a fraudulent transaction. The potential solutions to this risk are serialized one-time password generators.

Enhanced Web Single Sign-On (W-SSO) solutions are the most prominent choice to increase security on mobile phones. Also, step-up login features and device identification solutions will help address the increasing fraud.

**Trend #2: Increasing shift from rule-based systems to self-learning predictive models**
Currently, most web fraud detection (WFD) products are rule based, but advanced end users are increasingly seeking self-learning predictive models (mathematical models based on artificial intelligence) that discover fraud on their own.

While rule based products allow end users to update their models quickly enabling them to immediately respond to new threats and attacks, predictive models will provide additional patterns and trends to what analysts already know, thus improving the overall fraud detection rate. Hence, there is an increasing demand for products that combine both mathematically predictive models and rule based models.

Predictive model scoring systems also make it easier to set thresholds, enabling firms to monitor and adjust their false-positive and transaction-review rates leading to greater operational efficiency in fraud management.

**Trend #3: Increasing demand for an enhanced business user interface for alert management**
In order to counter increasing fraud, fraud specialists are seeking an enhanced business user interface for alert management.

One important requirement for many fraud specialists in such a business interface are transparent alerts (as these make it easier to understand the reasons for a particular alert). Also, the interface should be functionally convenient for these specialists to easily set and update rules, in order to address the latest threats and tactical requirements.

**Small and mid-size organizations do not emphasize advanced functionality that large organizations typically require.**

**Trend #4: Small and mid-size organizations seeking deployment and support simplicity in EFM products**
Ease of deployment and after-sales support are an important priority for organizations that have limited fraud management staff and support capabilities.

For small and mid-size organizations, ease of deployment, after-sales support, and predefined fraud detection rules and models form the key priorities while choosing an EFM product.

Also, small and mid-size organizations typically have limited budgets and prefer standard EFM products which are cheaper when compared to those which offer advanced functionality and complex models.

# 4 Effective Methods to Mitigate Fraud

## 4.1. Key Requirements

An effective fraud mitigation solution should revolve around operational efficiency, effective analytics, coverage, and real-time support. The following requirements have been identified by industry analysts[18] as the most critical for financial services institutions in fighting credit card transaction fraud:

- **Low False-Positive Ratios.** An effective fraud mitigation solution should have low false-positive ratios[19]. Higher ratios not only have an adverse impact on customer satisfaction but also increase the operational cost of managing fraud. An ideal fraud mitigation solution needs to balance customer satisfaction (by faster processing of the transactions) and minimizing the loss due to possible fraudulent transactions.
- **Real-time Transaction Support.** In order to decline credit and debit card transactions that are suspected to be fraudulent, a sub-second response is required. An ideal fraud mitigation solution (mainly used by organizations that need to detect time-sensitive transactions) should have this ability.
- **Entity Link Analysis.** To detect organized criminal activities, the relationships among various internal and/or external entities and their attributes (name, addresses, and national identification numbers) have to be carefully analyzed. Entity link analysis is the commonly employed method. A good fraud mitigation solution should include this critical ability in order to prevent collusive criminal activities. Once again, a low false-positive ratio is desirable here as higher false alarms will lead to an increase in the operational cost of managing fraud. Also, in order to efficiently leverage this feature, it is optimal to employ visualization techniques which can highlight suspect relationships.
- **Channel and Product-Specific Coverage.** For a single organization to be effective, different products and channels require different fraud detection algorithms and work flows. Hence it is very critical for a fraud mitigation solution to have the ability to adapt to multiple channels (such as online and in-person) and to different business products (such as credit cards and online payments).
- **Fraud Analytics and Intelligence.** An effective fraud mitigation solution should consist of embedded analytics and intelligence derived from rules and mathematically predictive models. It should also have the ability to profile accounts, users, and other internal/external entities. Higher fraud detection rates are achieved when incoming transactions are compared with the expected profile of a particular entity.

[18] Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities, Gartner, October 2010

[19] The ratio of non-fraudulent transactions blocked or rejected as they were wrongly classified as fraudulent transactions

**Effective fraud mitigation methodologies are those which prevent current fraud attacks based on the patterns seen in previous fraud attacks.**

## 4.2. Popular Methodologies

Effective fraud mitigation methodologies are those which prevent current fraud attacks based on the patterns seen in previous fraud attacks. Neural networks, adaptive analytics, customer alerts/out-of-band techniques, and customer-level views are popular in fighting the rising trend of global credit card transaction fraud.

### Artificial neural networks[20]

An artificial neural network is an adaptive system that changes its structure based on internal and external information flowing through the network during the learning, design and modeling phase. Currently, neural networks used to fight fraud in the financial services industry are computational models based on non-linear statistical data-modeling principles. These neural networks are used to model complex relationships between inputs, such as customer spend patterns or merchant behaviours, and outputs, like previous authorization decisions. They are also used to find patterns in data and which are compared to historical fraud patterns for analysis. While neural networks are used to find relationships and patterns, rules written by fraud specialists are applied to these relationships and patterns to either authorize or deny transactions.

### Analytics

Analytics is an important tool used by the financial services industry to fight fraud. Analytics are used to evaluate the transaction activity for a portfolio[21]. This evaluation is used to develop a set of rules for that portfolio to be applied in the authorization process. Fraud specialists use findings from these evaluations to frame rules mainly targeting the transaction characteristics such as size, nature and location of spending; transaction speed like the rate of card usage by the customer; and other known patterns. With regular maintenance, analytics will improve the performance of the neural networks since analytics can quickly spot changes in spend patterns and fraud trends.

### Alerts

Financial services institutions use alerts to enable cardholders to track their card usage in near real-time. Alerts are typically sent as an e-mail and/or SMS to cardholders but in some instances companies also make calls to inform the cardholder. Since a transaction must be successful in order to generate an alert, alerts happen after the fact and do not prevent the fraudulent transaction. But alerts do help financial services institutions block payments to fraudulent merchants claiming incorrect amounts and stop payments in cases where the transaction has happened without the knowledge of the consumer.

[20] David Kriesel, 2007, *A Brief Introduction to Neural Networks*, available at http://www.dkriesel.com

[21] Based on credit scores, spend & payment patterns and other relevant information, customers are grouped into portfolios for easier evaluation

While financial services institutions typically decide the rules for generating an alert such as the transaction amount or frequency, cardholders can also sometimes customize their own alerts. Fraud specialists and business analysts write sophisticated rules based on the latest fraud trends/attacks and then alerts are verified with the cardholder.

**Customer-level views**
Customer-level views identify the like spending patterns of different customers and group them together to monitor subsequent transactions. These methods are used to find suspicious behavior by risk scoring those groups across an organization's complete portfolio of products and brands. The fraud specialists can then take certain actions on the card usage of these individuals based on the verification results.

Finally, customer-level views also include identity-level fraud detection, which relates the individual consumer's identity characteristics with those of other consumers. This helps financial services institutions check for inconsistencies in details submitted by consumers such as the same SSN, phone or addresses across different applications.

### 4.3. Recent Developments in Fraud Mitigation

**Offline entity link analysis**
This solution utilizes robust social-network based analysis to identify unseen relationships between collaborative fraud entities. It is mainly used for offline analysis of broader customer and staff behavior and cannot be used to block fraud in real time. Also, once a fraudulent transaction is identified, these solutions can identify other entities that are connected to the fraud through social networks, and then risk score those entities to determine financial risk to the company.

**Device tracking**
Device tracking can track web-based devises such as PCs, mobile phones, gaming consoles, etc. and will initiate action when unexpected devices are used to conduct financial transactions. Upon identifying an unexpected device, the solution can force the customer to provide further authentication information and certain suspect devices can be blocked outright. This technology has the ability to track the device without creating a cookie or other component on the user's device since the cookie can potentially be modified or blocked. Finally, device tracking can be an important input to entity link analysis.

# 5 Conclusion

Despite the credit card industry's effort to fight fraud, global fraud losses are on the rise, driving an increase in the cost to fight fraud. In order to fight the growing fraud, financial services institutions are increasingly moving towards commercial EFM products as most in-house solutions are inadequate in addressing the new threats. Also, latest EFM products have the capability to process large transactional volumes and provide customizable rules that allow firms to update their models fast enough to address tactical requirements.

In the area of web fraud detection, advanced end users are increasingly seeking self-learning predictive models—such as mathematical models based on artificial intelligence—that that can run in parallel to the rule-based models, in order to improve fraud detection rates. These predictive model scoring systems also make it easier to set thresholds, enabling financial services institutions to monitor and adjust their false-positive and transaction review rates, leading to greater operational efficiency in fraud management.

Counterfeiting of cards through techniques like cloning has decreased with the introduction of EMV technology. However, EMV technology cannot address fraud in card not present (CNP) situations or in situations where PINs have been stolen or compromised[22]. The rate of adoption of EMV technology has been slow so far, and major markets like United States are yet to adopt this technology.

The most effective credit card fraud mitigation methodologies are those which prevent current fraud attacks based on the patterns seen in previous fraud attacks. Currently, neural networks combined with adaptive analytics seem to provide the most satisfactory credit card fraud detection capabilities. With regular maintenance, analytics will improve the performance of the neural networks since analytics can quickly spot the change in card portfolios spend patterns and fraud trends.

Recent developments in the area of fraud mitigation such as offline entity link analysis which uses social-network based analysis and device tracking that tracks web-based devices are complementing the existing solutions, thus improving the overall fraud detection rates of financial services institutions.

[22] EMV: the story so far, Banking & Payments Asia, May 2009

# References


1. *World Payments Report 2011*, Capgemini
2. *Global Card Fraud*, The Nilson Report, June 2010
3. PCI Standards Council, https://www.pcisecuritystandards.org/security_standards/
4. *True Cost of Fraud study*, LexisNexis, 2011
5. Credit card statistics, industry facts, debt statistics from www.creditcards.com
6. *2011 Identity Fraud Survey: Consumer Version*, Javelin Strategy & Research, February 2011
7. *Payments Fraud and Control Survey*, J P Morgan, March 2011
8. *Enterprise Fraud Management Predictions: 2011 and Beyond*, Forrester, December 2010
9. *Magic Quadrant for Web Fraud Detection*, Gartner, January 2010
10. *Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities*, Gartner, October 2010
11. *EMV: the story so far*, Banking & Payments Asia, May 2009
12. Smart Card Alliance, Smartcardalliance.org
13. David Kriesel, 2007, *A Brief Introduction to Neural Networks*, available at http://www.dkriesel.com

## About the Authors

**Vamsi Gullapalli** is a senior consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over three years of experience in strategy and business consulting for financial services clients across insurance, banking, and capital markets. Prior to joining Capgemini, Vamsi worked in a fixed income fund managing the treasuries portfolio.

**Sireeshkumar Kalli** is a lead consultant in Capgemini's Card Practice within the Global Financial Services Business Unit. He is a subject matter expert and project manager with over 11 years of experience in Credit Fraud & Risk Management in Cards and Lending domains.

**Ajay Vijay** is a senior consultant in Capgemini's Card Practice within the Global Financial Services Business Unit. He has over seven years of experience in Cards domain with a focus on Credit Fraud Management.

The authors would like to thank **Kripashankar Rajappa**, **Prasanth Perumparambil**, **Shantanu Fadnavis**, **William Sullivan**, **David Wilson**, and **Anuj Agarwal** for their overall leadership of this publication.

For more information, visit **www.capgemini.com/cards** or e-mail **cards@capgemini.com.**

## About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2010 global revenues of EUR 8.7 billion and employs around 112,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit **www.capgemini.com/financialservices**