WHITEPAPER

Payment Card Fraud – Building Walls to Beat Fraudsters' Ladders

sqs.com

Authors: Sudha Kiran Pentela (Principal Consultant)
Smitha Rao (Test Manager)
Subash Krishnan A (Lead Business Analyst)
Anish M.A (Business Analyst)
Nagarathnam Chandrasekar (Business Analyst)

SQS India BFSI Limited

Published: August 2015

SQS – the world's leading specialist in software quality

SUDHA KIRAN PENTELA

Principal Consultant
sudhakiran.p@sqs.com

Sudha Kiran Pentela has been with SQS since 2001 and is Principal Consultant in the Cards and Payments practice. His role involves handling various aspects of functional consulting, delivery and pre-sales such as developing strategies for testing, planning, business analysis and design, and providing operational support to ensure the success of various testing projects. As a Subject Matter Expert he has played a key role in many large cards and payments transformation programmes and projects. He has supported major Global 500 companies in the Cards and Payments processing sector, including Barclays Bank PLC (UK), Lloyds Banking Group (UK), Morgan Stanley (UK), GE Money (Germany, Denmark, Switzerland, Russia, UK and Singapore), First Data International (Singapore, Australia, Europe and the Americas) and TSYS International (Europe). Sudha Kiran is based in Chennai and holds a bachelor's degree in Mechanical Engineering from JNTU College of Engineering, Hyderabad.

SMITHA RAO

Test Manager
smitha.rao@sqs.com

Smitha Rao holds Project Management Professional (PMP) certification and a master's degree in Business Administration, and has been with SQS since 2004. Currently a Test Manager, she has an accomplished track record in managing various functional testing projects for leading global clients in the Cards, Banking and Treasury domains. Core competencies include end-to-end project management, strategy development and testing, business analysis and pre-sales in order to deliver tailored solutions to clients.

SUBASH KRISHNAN A

Lead Business Analyst
subash.krishnan@sqs.com

Subash Krishnan holds a bachelor’s degree in Engineering and a master’s degree in Business Administration. Having joined SQS in 2013, he is currently a Lead Business Analyst with an established track record in successfully implementing projects for leading clients in the Cards and Banking domains. Pri or to SQS, he worked for Infosys Technologies as Technical Lead in implementing AML solutions for AMEX, US.
His core competencies are business analysis, pre-sales and project management.

ANISH M.A

Business Analyst
anish.ma@sqs.com

Anish M.A holds a post-graduate degree in Business Administration backed up by 10 years of experience, predominantly in the Cards sector. He has previously worked for Standard Chartered, HSBC and Citibank handling various credit card processes. Having joined SQS as a Business Analyst in 2013 he has participated in a number of different projects which involve business analysis, preparation of scope documents, and defect & test management. He also played a vital role in integrating FALCON Fraud Manager into one of his recent projects.

NAGARATHNAM CHANDRASEKAR

Business Analyst
nagarathnam.c@sqs.com

Nagarathnam Chandrasekar has been with SQS since 2013 as a Business Analyst in the Cards practice. He has brought with him over 8 years of experience in the Banking and Cards domain, plus expertise in credit underwriting, cards pre and post issuance processes, and business & requirements analysis. He is currently working on the integration of a strategy management system with one of the largest card processing systems. Nagarathnam is a university rank holder with a master’s degree in Business Administration and is based in Chennai, India.

Contents

Management summary 4

Introduction. 5

Dimensions of card fraud. 6

Facts and trends 8

Key takeaways 9

Emerging trends 9

Combating fraud 10

Conclusion 12

References 13

Management summary

A discernible trend in global payments is the unabated growth of non-cash payments in every region. Correspondingly, most countries with a mature card market have experienced high fraud rates in recent years. Card fraud is a multi-billion pound problem and represents one of the biggest concerns among consumers.

Fraud has various dimensions and is not an undifferentiated phenomenon. It can occur in card-present or card-not-present environments using credit, debit or prepaid cards; it can arise in domestic or cross-border transactions and can be committed by customers, merchants, firm insiders or third parties.

Fraud is not static and keeps evolving. In recent years we have observed a sharp increase in card-not-present fraud in Europe. The delay on the part of US issuers to implement EMV-based systems has repercussions for issuers in other regions: European card issuers are now facing increased cross-border fraud losses in overseas markets, especially in the US. Trends also point to the emergence of Fraud as a Service (FaaS), where fraudsters join forces as a network to carry out cybercrimes in an organised manner.

Technological advancements in detecting and preventing fraud, coupled with the involvement of regulatory bodies, have started to show some promise in combating this practice. There are various established, intelligent Fraud Management solutions available on the market designed to detect and prevent fraud. However, combating fraud is a constant battle as fraudsters continuously attempt to beat the system.

In this whitepaper, we cover the various types of fraud, its dimensions, trends and concerns, and look at popular strategies to combat this process.

Introduction

Consumer use of electronic payment methods continues to grow strongly, wit h both mature and developing markets experiencing an increased use of cards year on year, both online and at point of sale. According to the World Payments Report 2014 [1], non-cash payments accounted for 366 billion transactions in 2013.

While much of the global payments industry benefits from this increased use of non-cash payments, the downside of this growth has been the rebound of fraud losses, despite the industry's best efforts to minimise consumer exposure. Globally, payment card issuers, merchants and their acquiring banks lost $ 14 billion to fraud in 2013 compared to $ 11.7 billion in 2012. Card issuers and merchants incurred 60 % and 40 % of those losses respectively.

Though the direct loss is estimated at $ 14 billion, the true cost of fraud is much higher considering both merchant costs (fees, penalties, replacement costs, etc.) and unquantifiable costs (trust/goodwill). LexisNexis [2] estimated that merchants lose an average of $ 3.08 per dollar (2014), up from $ 2.32 in 2011. Much of this is attributed to the increase in fraud through mobile channels, which costs merchants $ 334 for every $ 100 of fraud losses.

Card fraud continues to increase as fraudsters come up with innovative and organised hacking techniques that allow them to attack consumers, businesses and financial institutions via the payment channels available today. Though attempts are made to end all types of payment fraud, it continues to evolve. With the creation of new security technologies such as tokenisation, the industry can hopefully begin to be pro-active rather than reactive against payment fraud attacks.

Dimensions of card fraud

Card fraud has various dimensions and each of these can manifest itself in one or more combinations, giving rise to a multitude of potential fraud schemes. The various dimensions of card fraud are shown in Figure 1.

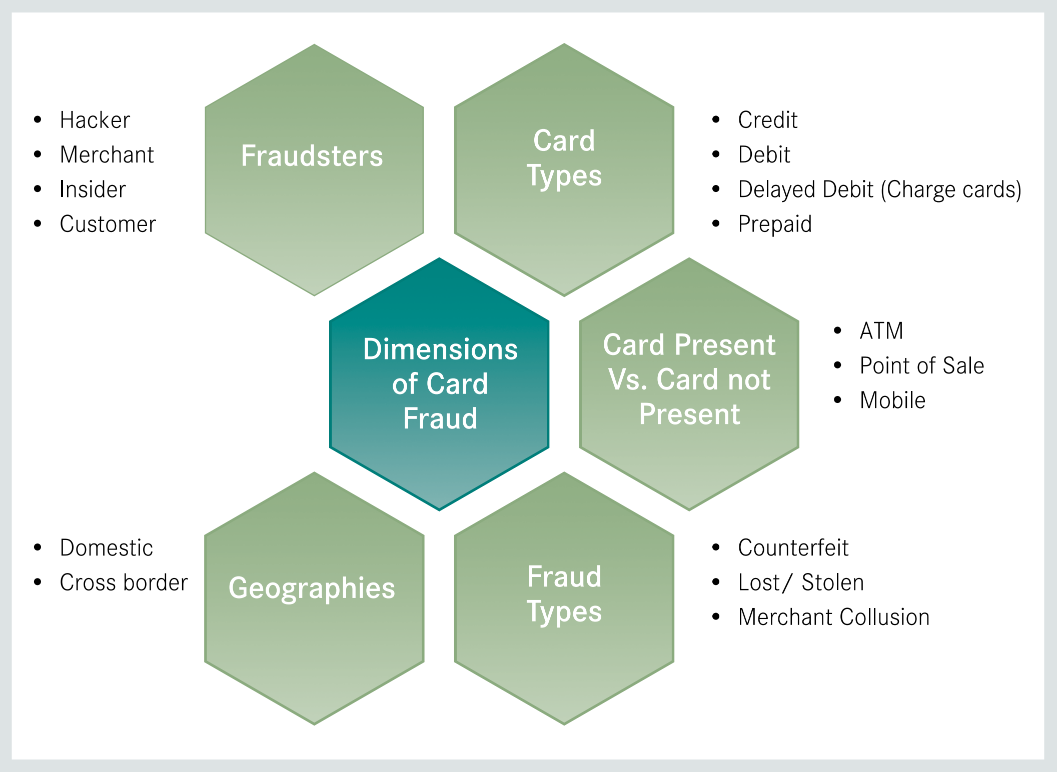

Figure 1: Dimensions of card fraud

Card fraud can happen at almost every stage of the card life cycle and the primary casualties are often the financial services institution, the merchant and the consumer. Each type of card fraud impacts each related stakeholder in a different way. In most cases, customer confidence is dented, issuer and acquirer reputations are at stake and the merchant has to go through detailed claims procedures. The impact of various card frauds on the different stakeholders is detailed in Table 1.

Stages in Card Life Cycle	Fraud Type	Issuer	Customer	Merchant	Acquirer
Application Processing	Application Fraud	1 5			
	Document Forgery	1 5			
Card Issuance	Courier Interception	2	4		
	Account Takeover	2	1		
ATM Usage	ATM Skimming		4		2
Point of Sale Usage	Skimming	1 2	1 4	1 3	2
	Counterfeit Cards / Cloning	2		1	
Online Usage	Phishing		1 4		
	Site Cloning		1 4	1	
	Malware	3			3
	BIN attack	2		1	
	Merchant Collusion			3	3

1 Financial Loss including customer communication cost / Shipping cost

2 Replacement of Cards/ Terminals

3 Loss of contract/ sensitive customer data

4 Tedious Dispute Management Process

5 Tightened application processing norms

Table 1: Card fraud types and their impact on different stakeholders

Facts and trends

Fraud shifts and migration are determined by the initiatives and responses across markets. Analysis and studies by regulatory bodies like the European Central Bank, the Federal Reserve in the USA and many other central banks across the globe, indicate an increase in both card-present and card-not-present (CNP) payments.

Table 2 analyses the fraud trends in three key markets in 2013 [3, 4, 5].

Parameters	Europe	USA	Australia
Fraud losses	Total fraud losses amounted to £ 450.4 million in 2013 - an increase of 16 % from 2012	The US accounted for 51 % of global card fraud losses in 2013 with total losses of $ 7.1 billion	Total fraud losses accounted for $ 304 million in 2013 up from $ 261 million in 2012 - an increase of 17 %
Top fraud type	Card-not-present fraud accounted for £ 301 million, followed by lost/stolen at £ 59 million and counterfeit at £ 43 million	Card-not-present fraud accounted for 45 %, followed by counterfeit and lost/stolen fraud at 37 % and 14 % respectively	Card-not-present fraud saw an increase of 19 % in 2013 at $ 219.7 million, followed by counterfeit fraud at $ 37.2 million
Domestic vs. cross-border fraud	Cross-border fraud outside the SEPA accounted for 25 % of total fraudulent transactions	The US saw a decrease of 12 % in cross-border card fraud	Cross-border fraud was higher than domestic fraud at $ 51 million in 2013
Most vulnerable card types	The share of delayed debit and credit card fraud in overall fraud remained at a higher level than that of debit cards	The overall number of compromised accounts increased by 9 % for debit cards, while remaining static for credit cards	Same as Europe
Cardholders impacted (5 years to 2012)	31 %	37 %	30 %
Data security focus	Data Authentication – Focus on making stolen data hard to use	Data Protection – Focus on making data hard to steal	Same as Europe

Table 2: Fraud trends in key markets

Key takeaways

- In Europe, the increase in card-not-present (CNP) fraud accounted for
    - 68 % of all fraud for delayed debit and credit cards
    - 48 % of all fraud for debit cards
    - 54 % of all fraud for all cards
- In the US, losses due to counterfeit cards amounted to $ 3 billion in 2013. The main reason for this is the non-adoption of Chip and PIN technology with far more magnetic stripe cards in use. EMV implementation is expected to reduce this figure to $ 1.8 billion; however there could still be an increase in CNP fraud
- The online shopping behaviour of Australian consumers has increased during recent years, which has in turn paved the way for fraudsters to target domestic and cross-border CNP transactions
- Any successful reduction in fraud, such as that driven by Chip & PIN, typically results in criminals changing their modus operandi to find a different weak spot, and fraud levels start to climb again in other areas. A good example is the implementation of EMV in Europe and Australia which has led to a reduction in counterfeit card fraud but resulted in increased incidents of CNP fraud

Fraudsters' centre of attention is mainly card-not-present (CNP) fraud, as opposed to other types of fraud. There is a real need to combat CNP fraud for m-commerce & e-commerce retailers.

Attacks by fraudsters on major retailers affected the shopping behaviour of customers, with 28 % of victims indicating that they avoided the particular merchant post-fraud.

Emerging trends

Fraud as a Service (FaaS)

One of the recent trends in the Payment Card industry is the emergence of Fraud / Cybercrime as a Service, allowing cybercriminals to execute attacks at a considerably reduced cost.

Services under FaaS include:

- **Research** – Vulnerabilities for sale, Exploit Brokers, Spam Services
- **Crimeware** – Professional Services, Malware Services, Exploits
- **Cybercrime Infrastructure** – Botnets, Hosting & Spam Services
- **Hacking** – Password Cracking, Denial of Services, Credit Card Information

Fraudsters use techniques like botnets, authentication bypass, SQL injection and a computer's running memory in addition to skimming, phishing, etc. to steal card information. They often provide their services on a fixed-rate fee or commission basis, to customers with little or no knowledge on how to execute a fraud / hack an account. Also, advances in the IT industry such as cloud computing afford opportunities for cybercriminals to offer these services on the cloud based architectures.

Credit cards – most popular item on sale in the underground economy

- Price for stolen card information ranges from $ 1 - $ 100
- Discounts offered on bulk purchases
- Potential worth of credit cards on sale was estimated at $ 5.3 billion/year

Source: Report on the Underground Economy by Symantec Corp [6]

Mobile Payments fraud [7]

Mobile Payments as a sector is starting to mature, with a high growth rate over the past few years. Around 32 % of merchants in the US have started to accept mobile payments including Apple Pay, PayPal and Google Wallet at the point of sale. However, mobile channels provide great potential/opportunities not only for organisations, but for fraudsters as well. Merchants say that m-commerce is as risky as traditional e-commerce. Tracking of fraud plays an important role in mobile channels for merchants and acquirers, as most fraud takes place in international rather than domestic transactions. Thus there is a requirement for more specialised tools to manage fraud that occurs via mobile channels.

Combating fraud [8]

Although technological advances, along with the involvement of regulatory bodies, have started to make some headway in combating fraud, most financial institutions find themselves constrained by the following issues:

1. Lack of standards for the computation of fraud losses, making it difficult for experts within banks to assess and apply appropriate counter-measures
2. Fraud departments working in isolation, resulting in fragmented strategies/solutions
3. Current anti-fraud strategies are more reactive than preventive. Without real-time transaction decision-making, the solution may not keep up with the pace of the fraudsters
4. Organisations should clearly understand fraud trends and design better processes to reduce the risk of fraud (prevention), discover fraud (detection) and take corrective actions (response).

Some effective methods to prevent and detect fraud have been listed below. These techniques/strategies could be implemented at business process level or at system level based on defined parameters.

1. **Customer screening** – Verifying customer data for any inconsistencies, and flagging fraud cases on a continuous basis; implementation of stringent KYC, AML norms
2. **Cardholder education** – Educating cardholders on handling card and PIN details, phishing, etc.
3. **Cardholder/card/transaction verification**
   - Cardholder verification: methods include signature, PIN, photo cards, etc.
   - Card authentication: methods that help to ensure that transactions are made using a genuine card - hologram, Dynamic Data Authentication, Combined Data Authentication in case of EMV cards
   - Transaction authentication methods like Cryptographic Validations, Multi-factor Authentication, 3D Secure, Verified by Visa (VBV) for e-commerce transactions
4. **Data security** – end-to-end encryption and tokenisation are the top choices for companies seeking to employ new emerging technologies to protect payment card and other critical data
   - End-to-end encryption is continuous protection of the confidentiality and integrity of transmitted data by encrypting it at the origin, then decrypting at its destination
   - Tokenisation replaces sensitive card data with unique ID symbols that retain all the essential data without compromising its security
   - Standards and guidelines like PCI-DSS and PA-DSS prescribe the norms for cardholder/card data storage and transmission
5. **Transaction screening** – rule-based systems like Fraudguard target transaction characteristics such as size, nature and location of spending, frequency of card usage and other known patterns, for transaction screening/evaluation purposes
6. **Neural & Bayesian networks** – data mining techniques for classification, clustering, generalisation and forecasting (predictions). These systems use patterns in data to separate legitimate from fraudulent transactions. Advanced applications such as FALCON use neural networks in addition to rule-based technology, while the FRACTAL application uses the Bayesian technique

Most of the Fraud Management Solutions available on the market consist of embedded analytics and intelligence derived from rules and predictive models. Testing of these solutions requires thorough understanding of business rules, scoring logic, authorisation flows and case management.

Live Example

SQS has helped many global clients (card processing service providers and end banks) in the integration and implementation of fraud management applications.

The client is a leading hybrid retailer, issuing both private label and scheme-branded cards in the Latin America region, with a card base in excess of 12 million. The client planned to use the advanced features of Falcon Fraud Manager (V6.3.1.0) for fraud detection & case management to provide a higher level of protection. The implementation involved:

- Initial proving, to ensure existing authorisation functionalities worked as expected
- Data validation of initial data feeds (batch and online) into Falcon for consistency & appropriate format usage
- Profile maturation – update of card and account profiles from both batch and real-time sources for a period of 90 days
- Configuration of fraud rules for testing
- Validation of authorisation decisions (approvals, declines and referrals) taken by Falcon based on the fraud scores & rules and case management

Extensive testing by SQS unearthed solution gaps and defects leading to design changes. The SQS team consistently maintained data precision for over 1 million records for performance testing. While more than 50 % of the defects resulted in code changes, over 70 % of the defects were in a priority category. The client applauded the SQS team, stating "together you have found a massive amount of defects .... exposing weaknesses in the code, you are the gatekeepers for Production"

Conclusion

The continuous increase in global card fraud losses is driving businesses to fight back with robust fraud mitigation strategies, to develop and refine fraud controls, and also to provide consumers with tools and knowledge to prevent, detect and resolve fraud. The industry is moving towards enterprise-wide solutions that are capable of processing large volumes of transactions in real time. Neural networks, coupled with adaptive analytics, seem to provide the most satisfactory card fraud detection capabilities.

As banks adopt and amend their fraud detection and prevention processes, fraudsters too shift to weaker links, identify newer vulnerabilities, and manage to 'beat the system' by building a higher ladder. As Frank Abagnale Jr. in the movie 'Catch Me if You Can' says, "you're gonna have to catch me first!". For financial institutions, it's a constant battle to keep up with 'innovative' fraudsters. Tackling payment card fraud requires a holistic, layered and multi-pronged strategy without compromising on the customer experience.

References

[1] Capgemini, RBS (2014). World Payments Report 2014.

[2] LexisNexis (2014). True Cost of Fraud^{SM} Study.

[3] Australian Payments Clearing Association. http://www.apca.com.au

[4] European Central Bank. Report on Card Fraud.

[5] Nilson Report (2013). Business Intelligence.

[6] Symantec Corp (2008). Report on the Underground Economy.

[7] Kount, The Fraud Practice and CardNotPresent.com (2015). Mobile Payments & Fraud: 2015 Report.

[8] C. Brown (2010). Stopping Card Fraud - An industry guide from ACI.

Irrespective of the care taken in preparing the text, graphics and programming sequences, no responsibility is taken for the correctness of the information in this publication.

All liability of the contributors, the editors, the editorial office or the publisher for any possible inaccuracies and their consequences is expressly excluded.

The common names, trade names, goods descriptions etc. mentioned in this publication may be registered brands or trademarks, even if this is not specifically stated, and as such may be subject to statutory provisions.

SQS Software Quality Systems AG
Phone: +49 2203 9154-0
Fax: +49 2203 9154-55
info@sqs.com | www.sqs.com