Payments Newsletter

Towards a more secure payments ecosystem

August 2018

Foreword

Dear Readers,

It is my pleasure to bring to you the latest edition of our payments newsletter, where we take a closer look at the risks that are associated at various touchpoints across the payments ecosystem. We discuss important security measures and present a risk management framework that firms can establish to offer a seamless and more secure transacting environment.

I hope you will find this to be a good and insightful read.

For further details or feedback, please write to

vivek.belgavi@pwc.com or mihir.gandhi@pwc.com

Introduction

The rapid adoption of digital payments in India and the entry of new payment channels have made risk management an important focus area in the payments ecosystem. Any breach in security of payments is likely to affect the diligently built confidence of customers. As the government pushes for wider adoption of digital payments across multiple use cases, incidences of fraud may make customers wary of security within payment systems and thus it is necessary for all participants in the ecosystem to continuously make efforts to make payments security and risk management a priority for their business.

With stakes getting high to secure payment systems, all players involved – banks, regulators, card networks, e-commerce companies, FinTechs are actively working to protect their customers. We look at steps being initiated towards more enhanced risk & security measures in payments-

1 Regulators across the world, with their guidelines on authentication, data storage & privacy, customer identification & verification etc. are playing an active role at an overall level to prevent breaches. With respect to data privacy, implementation of PSD2 & GDPR in EU & EEA and recommendation of Justice Srikrishna Report in India will change the way companies collect & process personal data, with control over data sharing resting with individuals. Similarly, to address privacy concerns around Aadhaar, UIDAI has mandated use of 16 digit Virtual ID (VID) instead for Aadhaar for customer verification.

2 With growing digital transactions, banks are exploring near real-time data analytics and block chain combined with cognitive learning to mitigate risks arising in payments systems. Fintech and technology companies are developing solutions based on adaptive and step-up authentication for e-commerce transactions. Banks and financial institutions have initiated educational programs for customers and employees to forewarn about various risks in the system and basic steps to mitigate the same. To reduce repudiation risk, banks are encouraging customers to opt for digital signatures while making high-value inter-bank transactions through net banking. Traceability of transactions in blockchain reduces repudiation risk of the transacting parties and thereby has become one of the key points for the financial institutions to further explore this technology.

3 Even though PIN based transactions have gained traction globally, push for NFC based payments have witnessed encouraging response in countries like Australia, Canada, Sweden & Japan. However, there have been a few security concerns over NFC based payments such as capturing details by bringing POS terminals close to customers in crowded areas. This has prompted card schemes to offer tokenization to banks and payment service providers, which is an attempt in the right direction to make transactions more secure. Recent Government of India communication to banks on issuing NFC based cards is going to provide a fillip to these form factors. Card manufacturing companies have developed biometric based cards and one such company is also conducting a pilot project in Japan.

Overall, apart from the direct financial impact of fraud, costs related to prevention and revenue/opportunity loss due to fraud should also be attributed to the total cost of risk management for an organization. The strategy of how to manage these costs vary greatly on the type of industry, business model, geography, payment methods and type of fraud involved.

The table below summarizes the current dominant payment instruments/ channels and efforts made by banks to mitigate the associated risks -

Dominant payment Instruments/ Channels	**Risk factors**	**Mitigation steps**
ATM/POS	➢ *Card skimming & cloning* ➢ *Malware Attack* ➢ *Network attack*	✓ *PoS upgraded to accept Chip + PIN* ✓ *ATMs being upgraded to read EMV Chip Cards* ✓ *ATMs being upgraded with latest version of Windows OS* ✓ *Segregate ATM network from corporate/branch network*
Cards	➢ *Card skimming & cloning* ➢ *Vishing*	✓ *Magnetic Stripe cards getting replaced with EMV chip cards* ✓ *Customer education on card safety features*
Mobile payments	➢ *Malicious Apps* ➢ *Rooted Device*	✓ *Updated operating system* ✓ *Updated applications* ✓ *Avoid downloading untrusted applications*
Internet Payment Gateway	➢ *Vishing* ➢ *Untrusted websites* ➢ *Cookies* ➢ *Data leakage*	✓ *Updated OS and browser* ✓ *Updated anti-virus* ✓ *Using SSL sites for transactions* ✓ *Clearing cookies on a regular basis* ✓ *Strong Encryption*
New age payment modes –UPI, QR etc	➢ *Incorrect implementation of application* ➢ *SIM cloning* ➢ *Data theft through tampered POS*	✓ *Transaction limits* ✓ *Compliance to PKI and HSM requirements* ✓ *Incident and event monitoring* ✓ *Regular code and tech design review*

There have been a quite a few case studies where financial institutions and payment companies across the globe have deployed advanced security measures for safer and more secure payment transactions.

Case study I: Addressing cross-border money laundering

Problem Statement: A large global bank had faced massive penalties due to its failure to control money-laundering.

Solution: To ensure compliance in the future at manageable costs, it implemented a solution from a firm specialized in Anti-Money-Laundering. The solution helped the bank reduce number of false positives by 20%, without reduction in number of cases reported for suspicious activity. This saved the bank thousands of hours in investigation of compliance risks and was able to meet many of the required regulations, thereby saving hefty monetary penalties

Case study II: Upgrading fraud detection system

Problem Statement: A leading bank in New Zealand was impacted by a sudden spike in fraud volumes.

Solution: It found that its point- based fraud detection system was detecting only a fraction of the fraud attempts launched against the bank. It worked with a leading solution provider to upgrade its systems to detect patterns in behavior of banking customers and use subtle deviations for identifying frauds. This provided speed and agility to the bank in spotting fraud schemes and attacks before they occurred and better adapt its defenses to new fraud threats.

Case study- III: Addressing customer frauds

Problem Statement: One of the leading payment gateways in Turkey was facing huge losses of fraudulent chargebacks claimed on credit card transactions.

Solution: It realised that a significant portion of the chargebacks was due to friendly frauds. Customer carried out transactions themselves and after receiving items, claimed refund. To evaluate such transactions, it implemented solution from a new age technology provider. It helped to identify whether a transaction is fraudulent or genuine based on a trust score. This score was generated through machine learning algorithms, a user's browsing behaviour analysis, device fingerprinting, location profiles and other evaluation parameters. The PG was able to improve on the decline rate by 50% and fraud chargebacks subsequently decreased by 65%.

Assessing Risks from new technologies

As players in the payments industry launch new instruments to facilitate payments along with ramping up the acceptance points, it also increases associated potential risks and threats to data privacy. This has an impact on customer confidence on the payment ecosystem. Some of the scenarios which pose risk are illustrated below -

Device Capability	*Devices have limited memory and processing power to consume well established security protocols for today's standards. This makes it difficult to push regular security updates to devices.*
Data Leakage & Privacy	*New age payment touchpoints have the potential to generate large amounts of data, representing a potential target for cyber criminals. Stolen data is likely to contain personal information that can then be used for unlawful surveillance and tracking users.*
DDoS Attacks	*Default credential settings and open remote access make it easier for attackers to take over the device remotely. Typically, IoT devices require minimal or no user interaction, which makes it even more difficult for users.*

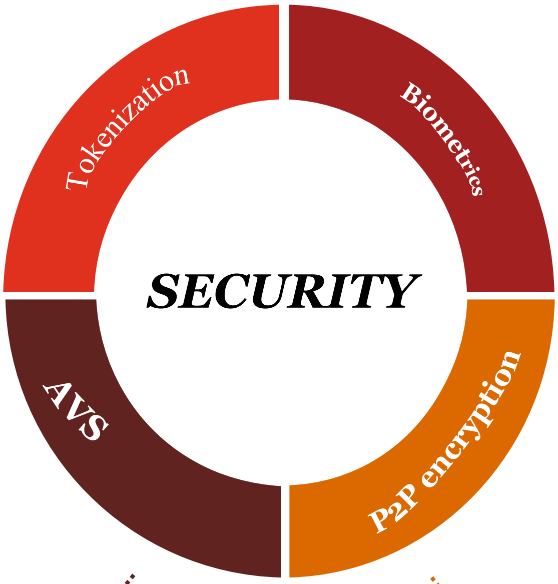
It is hence critical to ensure adequate risk and security measures are implemented to ensure adoption of payment instruments. However, layers of security added by financial institutions to mitigate risk at times result in non-delivery of OTP, technical declines & time-outs. This results in poor customer experience and in extreme cases, customer never returns to complete the transactions. Some e-commerce websites are using APIs or directly integrating with financial institutions to tackle transaction drop. However, scope of further improvement still exists and to address these challenges, firms are looking at deploying convenient payment options combined with various safeguards, few of which are illustrated below –

Tokenization

It appears to be the most preferred approach for securing payment account information in IoT and contactless payment transactions. The length of time a token remains valid is typically based on the level of perceived risk. Tokens in high risk environments will have a shorter validity period.

AVS

Address Verification Service requires customers to provide the billing address associated with their credit card. When the address on the card matches with the one in bank's documents, the transaction will go through. It is typically used for segments/ areas with higher risk



Biometrics

This security method relies on biological identification measures that are unique to a particular individual, such as fingerprint scanning, iris/retina scanning, facial imaging, vein patterns, voice recognition, finger/hand geometry, DNA matching, and ear, gait, and/or odor recognition.

P2P encryption

P2P encryption is a payment security measure that instantly converts customer details into a one-time code. Encryption can help satisfy regulatory requirements imposed by PCI DSS, HIPAA-HITECH, GLBA, ITAR and the upcoming EU Data Protection Regulation.

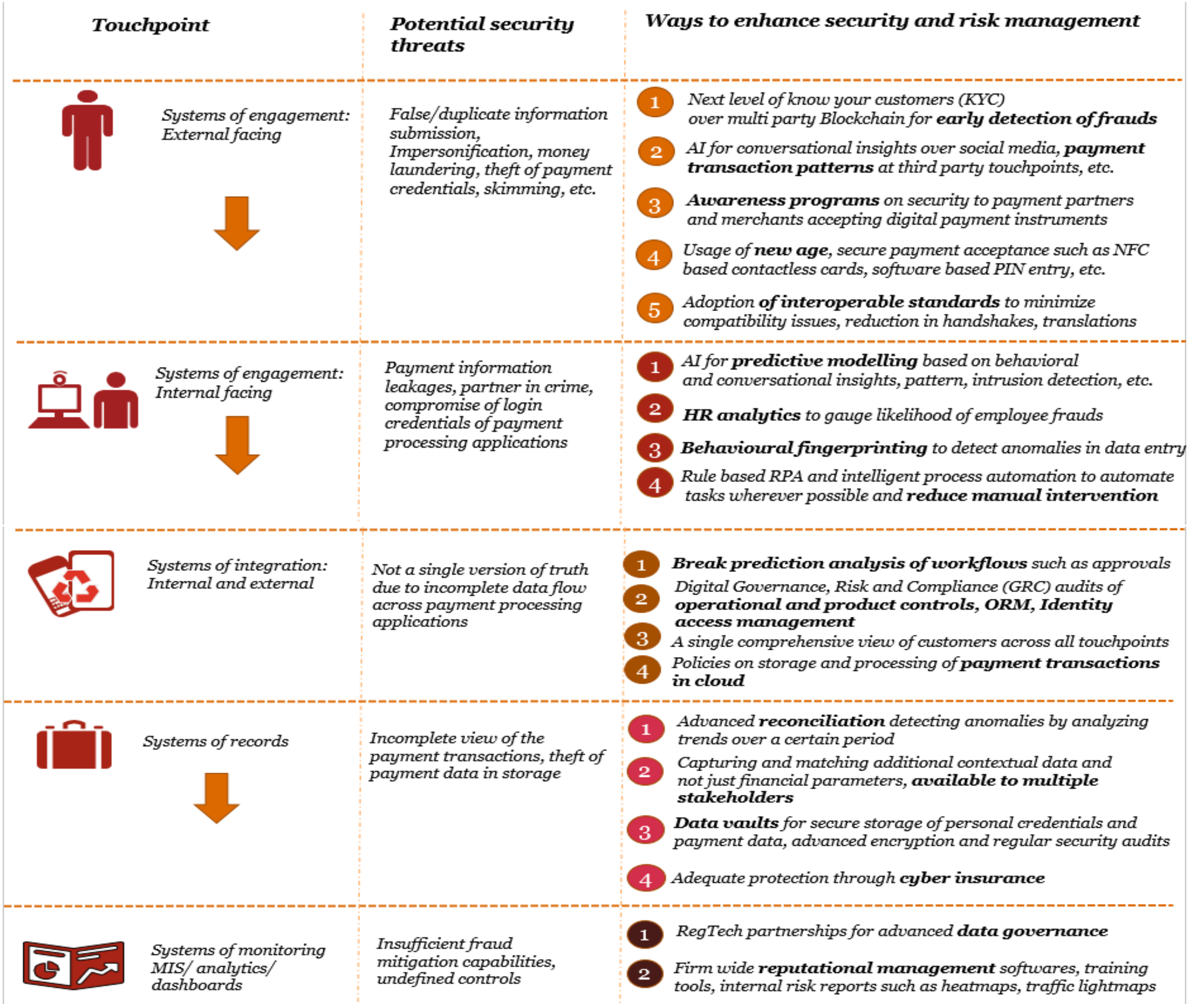
Towards a mature risk management framework

To continuously secure systems against ever-increasing sophisticated attacks, organizations have to think beyond the obvious in deploying security framework. A change at the organization level is critical to support new age systems deployed by banks. Illustrated below are a few areas which firms can evaluate, in order to be future ready.

Enhancing scope of strategic partnerships

Last few years have witnessed multiple strategic partnerships between financial institutions and firms in consumer-facing areas such as new age payment instruments, mobile products, trading and insurance products. There is a huge scope to partner with firms offering new-age solutions in areas such as security, data privacy and fraud risk management. These firms leverage power of big data, artificial intelligence and advanced predictive modelling to detect security risks and frauds at various touchpoints in the payment lifecycle, at early stage and help mitigate them.

A few areas where firms can enhance the security of the entire payment ecosystem are:



Touchpoint	***Potential security threats***	***Ways to enhance security and risk management***
Systems of engagement: External facing	*False/duplicate information submission, Impersonification, money laundering, theft of payment credentials, skimming, etc.*	1 *Next level of know your customers (KYC) over multi party Blockchain for* ***early detection of frauds*** 2 *AI for conversational insights over social media,* ***payment transaction patterns*** *at third party touchpoints, etc.* 3 ***Awareness programs*** *on security to payment partners and merchants accepting digital payment instruments* 4 *Usage of* ***new age****, secure payment acceptance such as NFC based contactless cards, software based PIN entry, etc.* 5 *Adoption* ***of interoperable standards*** *to minimize compatibility issues, reduction in handshakes, translations*
Systems of engagement: Internal facing	*Payment information leakages, partner in crime, compromise of login credentials of payment processing applications*	1 *AI for* ***predictive modelling*** *based on behavioral and conversational insights, pattern, intrusion detection, etc.* 2 ***HR analytics*** *to gauge likelihood of employee frauds* 3 ***Behavioural fingerprinting*** *to detect anomalies in data entry* 4 *Rule based RPA and intelligent process automation to automate tasks wherever possible and* ***reduce manual intervention***
Systems of integration: Internal and external	*Not a single version of truth due to incomplete data flow across payment processing applications*	1 ***Break prediction analysis of workflows*** *such as approvals* 2 *Digital Governance, Risk and Compliance (GRC) audits of* ***operational and product controls, ORM, Identity access management*** 3 *A single comprehensive view of customers across all touchpoints* 4 *Policies on storage and processing of* ***payment transactions in cloud***
Systems of records	*Incomplete view of the payment transactions, theft of payment data in storage*	1 *Advanced* ***reconciliation*** *detecting anomalies by analyzing trends over a certain period* 2 *Capturing and matching additional contextual data and not just financial parameters,* ***available to multiple stakeholders*** 3 ***Data vaults*** *for secure storage of personal credentials and payment data, advanced encryption and regular security audits* 4 *Adequate protection through* ***cyber insurance***
Systems of monitoring MIS/ analytics/ dashboards	*Insufficient fraud mitigation capabilities, undefined controls*	1 *RegTech partnerships for advanced* ***data governance*** 2 *Firm wide* ***reputational management*** *softwares, training tools, internal risk reports such as heatmaps, traffic lightmaps*

Rapid adoption of new age payment instruments will continue to pose challenging security questions to firms. In order to protect the customer and ensure that their confidence in the payment ecosystem is maintained, stakeholders need to invest in newer and safer tools and technologies. They also need to educate their partners to develop a mature risk management framework which will address risks associated with all new age payment products. As it is always said "Risk cannot be eliminated, it can only be mitigated", it is necessary to continuously assess risks and provide a safe, secure and future-ready transacting environment.

(With inputs from Neha Jaeel, Shekhar Lele, Kanishk Sarkar, Arun Suresh, Jaya Gupta, Amol Bhat, Vivek Rawell)

Payment Technology Updates

PayThink Wearables open a new door for payment fraud

PaymentsSource

The evolution of wearable devices is taking place at a staggering rate. From simple fitness trackers to tethered and stand-alone smartwatches, a tremendous amount of sensitive personal and financial information is being passed from device to device, device to cloud and wrist to wrist, putting consumer privacy and security—as well as enterprise data—at risk.

(Read More)

Payment Threats and Fraud Trend Report

European Payment Council

The threats trends report reflects the recent development concerning security threats and fraud in the payments landscape over the past year.

(Read More)

IoT and Payments: Current Market Landscape

Secure Technology Alliance

The Internet of Things (IoT) is growing rapidly—8.4 billion connected "things" are forecast to be in use in 2017. That number is expected to increase to 20.4 billion in 2020, 1 and starting in 2017, the IoT market is projected to be worth more than $1 billion annually.

(Read More)

12 Biggest Security Threats to Payments

ACI Universal Payments

Consumers ask a lot of you in terms of convenience, speed and, above all, security. This puts the pressure on you to offer a pain-free consumer experience that is also highly secure. And when you accept payments, you need to secure all parts of your organization.

(Read More)

Do Contactless Payments Pose a Greater Fraud Risk?

FICO Blog

The more likely potential threat of contactless is actually more complicated, and involves "disowned" transactions where the consumer fails to recall a transaction.

(Read More)

How Voice Biometric Technology is Preventing Payments Fraud

Credit Union Times

Payment companies are looking to reduce fraud, but it can be difficult to spot suspicious activity. One of the most common ways a fraudster can impersonate a customer is by calling the telco operator to request to port a number from another operator.

(Read More)

Please contact

For more information, please contact:

Vivek Belgavi
Partner- Financial Services and India FinTech Leader

Tel: +91 9820280199
Email: vivek.belgavi@pwc.com

Mihir Gandhi
Partner and Leader – Payments Transformation

Tel: +91 9930944573
Email: mihir.gandhi@pwc.com