WORKING GROUP ON SECURING CARD PRESENT TRANSACTIONS

REPORT AND RECOMMENDATIONS

MAY 31, 2011

Table of Contents

Acknowledgements

The working group would like to acknowledge the contributions of the following groups and individuals:

1. Mike Hendry (Payment Systems Consultant) for sharing his personal experience and learnings from his global assignments

2. Stakeholders from various companies in this space for their time and sharing their experiences / understanding - Harpal Singh, Verifone India; Rajesh Bansal, UIDAI; Amit Kakatikar Oberthur India

3. The VISA Asia Pacific team – Murugesh Krishnan and Manoj Sugathan for their valuable inputs on global case studies, managing large scale migrations and fraud trends

4. Representatives from Axis Bank who though not in the formal working group, joined the discussions and actively participated

5. Certain representatives from the participating banks deserve special mention:
   a. Venkata Suresh, ICICI Bank for his perseverance in ensuring industry challenges and business priorities were fully considered. We also thank Vinay Balse, ICICI bank, Sumit Chopra, First Data for their contributions
   b. Ramesh Krishnamoorthy, Standard Chartered Bank for his extraordinary diligence and valuable inputs on fraud risk
   c. Murali Manohar, VISA in ensuring global representation from the VISA team and contributing so much more
   d. Dilip Asbe, NPCI for his technical and implementation assessments. We also thank Gowri Narayanan for sharing his Europe experiences
   e. Chayan Hazra, MasterCard for his energy and enthusiasm in all discussions
   f. Rajanish Prabhu and Navtej Singh, HDFC bank in bringing in the balanced debit/credit perspective and the industry knowledge
   g. Richhpal Singh, SBI for sharing his rich experience and specifically ensuring the diverse priorities of the participants is a strong consideration. Rajesh Vaish for his inputs on emerging technologies
   h. VS Ramarao, Union Bank for his active participation and balanced views
   i. K Ramachandran, Corporation Bank for his active participation
   j. Subbalakshmi Shirali, Shamrao Vithal Cooperative Bank for her diligent feedback on the report
   k. Manesh Nair, American Express for his process inputs and understanding of the acquiring infrastructure
   l. Siddharth Mehta, Citibank for his domain understanding of the acquiring space. B Umaa, Citibank for her administrative support
   m. Radha Somakumar, RBI – for being the “check and balance” in the group and more importantly ensuring that all deliverables of the group lived up to her high standards

6. Last but certainly not the least, Shri G Padmanabhan, RBI for his direction, guidance and in clearly setting the focus for the group. Special thanks to K Sivaraman and K Vijaykumar from RBI for their support

Acronyms and Definitions

2FA	Two Factor Authentication
AOD	Account Opening Documents
ATM	Automated Teller Machine
BIN	Bank Identification Number
Bps	Basis Points
CDA	Combined DDA/Application Cryptogram Generation (CDA)
CIBIL	Credit Information Bureau (India) Limited
CST	Central Sales Tax
DDA	Dynamic Data Authentication
DES	Data Encryption Standards
DUKPT	Derived Unique Key Per Terminal
EDC	Electronic Data Capture
EPI	Euro Pay International
EMV	Euro pay MasterCard Visa
FTS	Fraud to Sales Ratio
HUF	Hindu Undivided Family
IATA	International Air Transport Association
ICC	Integrated Circuit Card
ISO	International Standardization Organization
IVR	Interactive Voice Response
KYC	Know Your Customer
MCI	Master Card International
MPR	Merchant Payment Report
MSD	Magnetic Stripe Data
NFC	Near Field Communication
NPCI	National Payments Corporation of India
OTP	One Time Password
PAN	Permanent Account Number
PCIDSS	Payment Card Industry Data Security Standards
PIN	Personal Identification Number
POS	Point of Sale
RSA	Rivest, Shamir and Adleman (inventors of the RSA cryptosystem)
SDA	Static Data Authentication
SMS	Short Message Services
TLE	Terminal Line Encryption
UID	Unique Identification
UIDAI	Unique Identification Authority of India
UKPT	Unique Key Per Terminal

Acquirer	Also referred to as “acquiring bank” or “acquiring financial institution.” Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric
Authorization	Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Cards Skimming	Card skimming is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. The scammers try to steal your details so they can access your accounts. Once scammers have skimmed your card, they can create a fake or 'cloned' card with your details on it. The scammer is then able to run up charges on your account. Card skimming is also a way for scammers to steal your identity (your personal details) and use it to commit identity fraud. By stealing your personal details and account numbers the scammer may be able to borrow money or take out loans in your name.
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the

	decryption process (the inverse of encryption) against unauthorized disclosure.
Encryption Algorithm	A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again.
Eavesdropping	Network Eavesdropping also known as Network Sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, pin, session tokens, or any kind of confidential information. The attack could be done using tools called network sniffers. These tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling.
Host	Main computer hardware on which computer software is resident.
Host Spoofing	Host spoofing is a malicious individual or program that impersonates a trusted host to gain access to a network, take over a user's web browser, impersonate a trusted source or even spoof trusted websites. It is a common method used by spammers and other scammers.
Information Security	Protection of information to insure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
IP	Acronym for “internet protocol.” Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address	Also referred to as “internet protocol address.” Numeric code that uniquely identifies a particular computer on the Internet.
Issuer	Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as “issuing bank” or “issuing financial institution.”
Key	In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to ciphertext.

	The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message.
Key Management	In cryptography, it is the set of processes and mechanisms which support key establishment and maintenance, including replacing older keys with new keys as necessary.
Magnetic-Stripe Data	Also referred to as “track data.” Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
Malicious Software / Malware	Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Merchant	a merchant is defined as any entity that accepts payment cards bearing the logos of American Express, Discover, JCB, MasterCard or Visa as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
Monitoring	Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
Network	Two or more computers connected together via physical or wireless means.
Password	A string of characters that serve as an authenticator of the user.
Patch	Update to existing software to add functionality or to correct a defect.
Payment Application	Any application that stores, processes, or transmits cardholder data as part of authorization or settlement

PIN	Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.
POS	Acronym for “point of sale.” Hardware and/or software used to process payment card transactions at merchant locations.
Replay Attacks	A breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. For example, messages from an authorized user who is logging into a network may be captured by an attacker and resent (replayed) the next day. Even though the messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid logon messages is sufficient to gain access to the network. Also known as a "man-in-the-middle attack," a replay attack can be prevented using strong digital signatures that include time stamps and inclusion of unique information from the previous transaction such as the value of a constantly incremented sequence number.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.
Smart Card	Also referred to as “chip card” or “IC card (integrated circuit card).” A type of payment card that has integrated circuits embedded within. The circuits also referred to as the “chip,” contain payment card data including but not limited to data equivalent to the magnetic-stripe data.
Transaction Data	Data related to electronic payment card transaction.
Two-Factor Authentication	Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

Terms of Reference

Card Present Transactions (transactions at POS and ATMs) constitute the major proportion of card based transactions in the country. Currently, transactions using cards at POS do not require additional authentication in majority of the cards. Further, data stored in magnetic stripe is vulnerable to skimming. Increasing confidence of the customer for using POS channel would require securing of these transactions through implementation of authentication in the short run and prevent counterfeiting of cards by migrating to chip and PIN in the long run. Considering the importance of this process, Reserve Bank of India (RBI) has constituted the Working Group with the following terms of reference:

i. To examine all aspects related to use of cards at POS and ATMs and recommend action plan for enabling, additional authentication of transaction using existing cards in a cost effective manner. The plan should enable implementation of the process within 6 months.

ii. To examine the merchant enrollment and monitoring process currently in practice from fraud vulnerability perspective and recommend measures to address these risks.

iii. To examine the cost aspect associated for migrating the infrastructure for enabling issuance and acceptance of Chip and Pin cards, and recommend a migration plan with specific timeframe for migrating all components associated. The plan should enable complete migration within 3 years.

The Working Group examined the following aspects as part of the process to arrive at the final recommendation:

1. *Existing payments infrastructure in the country*
2. *Solutions available to secure Card Present transactions and prevent skimming (covering both current mass adopted technologies and emerging technologies)*
3. *Solutions were evaluated across multiple dimensions including: Customer experience, Execution challenges, Business Challenges, Costs*
4. *Experiences in other markets*
5. *Inputs from other partners / service providers the ecosystem*
6. *Residual risks and new risks which emerge based on the final recommendation were understood and tabled – mitigants to manage the same also presented*

Problem Definition

Industry Size

The industry size (defined as total credit and debit card spends value) is approximately Rs. 1,13,000 crores (includes ecommerce, IVR, MOTO transactions from Mar '10 to Feb '11). The total credit and debit card POS spends value is Rs. 88,000 crores. ATM cash withdrawals are Rs. 10,91,115 crores. The number of debit cards is 24 crores and the number of credit cards is 1.8 crores. The total number of POS terminals is 5.6 lakhs and the number of ATMs is 70,000. *Figures as of Feb '11*

(Refer APPENDIX A for more details)

Point of Sale (POS) - Fraud Levels

In the context of terms of reference, two categories of frauds are relevant: Lost & Stolen card fraud and Counterfeit card fraud.

The total industry lost & stolen and counterfeit card fraud is Rs. 13 crores. The fraud to sales ratio is approximately 1.4 basis points (bps). However, a trend in counterfeit card fraud is that counterfeiting typically happens when customers travel internationally. The POS fraud summary details are as below:

	Fraud (INR crores)	Fraud (Frauds to Overall card spends - basis points)
Lost & Stolen card fraud	5	0.5 bps
Counterfeit card fraud	8.2	0.9 bp

Table 2 A

Note: Data is industry-wide annual fraud data. The frauds numbers are based on the numbers reported by banks to Visa and MasterCard.

	Domestic Fraud to Sales	International Fraud to Sales
Credit Cards	1.06 bps	28.28 bps
Debit Cards	0.19 bps	8.44 bps

Table 2B

ATM - Fraud Levels

Currently, banks separately report credit and debit card frauds. However, channel-wise classification is not available.

While the current fraud levels are low, the following considerations emerge:

1. *Early cases of domestic counterfeit and skimming are being observed. Currently, Counterfeit fraud is more prevalent internationally.*
2. *Strong case to treat domestic and international spends differently (Table 2B)*

Global Experience

Magnetic Stripe Card Countries

USA & China: USA and China are two examples of large countries that continue to issue magnetic stripe cards. In the US, the resistance to change stems primarily due to two reasons: Cost of migration to EMV as profitable revenue channels associated with current interchange fees do not offset the cost of re-carding. China has strong legal framework to handle financial frauds, which acts as a deterrent to fraudsters.

EMV Chip Card Countries

Regulatory Mandate

Most countries have migrated to chip card or chip card & PIN based on regulatory mandate.

Europe: Initial migration to chip cards in Europe took place to address high communication cost. Over time due to increase in counterfeit card frauds and due to SEPA (Single Europe Payment Association) mandate, most of the countries migrated to EMV Chip Card and PIN.

Malaysia: Malaysia migrated to EMV chip card with signature in 2005 to address counterfeit frauds and to comply with regulator mandate. Post migration, domestic counterfeit fraud in Malaysia had reduced drastically. However, international counterfeit fraud is still a concern due to usage of these cards as magnetic stripe cards in non-EMV markets. Malaysia has a regulator mandate for EMV Chip Card and PIN from January 2015 as lost or stolen card frauds have increased significantly.

UK: EMV Chip Card issuance commenced from 2005. Issuance of EMV Chip Card and PIN commenced from February 2006 as per regulator mandate. UK, similar to Malaysia, had seen significant reduction in domestic counterfeit fraud.

Singapore: Singapore had migrated to EMV chip cards from beginning of 2011 due to regulator mandate.

Industry Initiative

Australia & New Zealand: Australia and New Zealand have started issuing EMV chip cards for new and renewal cards as part of industry initiative. Both the countries propose to completely migrate to EMV chip from 2013 & 2014 respectively.

Brazil & Mexico: Few banks are implementing EMV Chip card issuance pilot projects to counter high counterfeit card fraud.

However, the readiness of ATMs to accept EMV Chip Card varies across the globe.

Refer APPENDIX B for more details on global EMV Chip Card Issuance & Acceptance. APPENDIX C for Inference derived from stress tests conducted.

Some key considerations:

Migration timelines vary from 4-6 years depending on size of industry

Fraud moves to the weakest link – RBI's move in securing Card Not Present Transactions first has ensured industry is well placed.

Fraud typically migrates from current fraud havens as- and- when these countries put in place controls to neighbouring countries. Malaysia and Singapore have implemented anti-skimming and second factor controls recently.

Indian Context

PIN as a second factor authentication

Certain issuers such as Citibank and SBI issue maestro debit cards. Maestro debit cards are magnetic stripe cards that require a PIN to be entered at POS terminal. Besides maestro, Citibank also issues debit cards that do not require PIN for POS transactions. Citibank's experience has been that card usage levels are significantly lower when PIN is required to be entered at POS terminal.

EMV Chip Issuing Infrastructure Readiness

Over 99% of the total cards issued in India are magnetic stripe cards. Currently, few large issuing banks like Citibank, ICICI Bank, HDFC Bank and SBI are issuing EMV chip cards. These banks are issuing chip cards typically to customers who frequently travel internationally and to customers who have high credit limits. All these cards are used as Chip and Signature. None of the issuing banks have started issuing Chip and Pin Cards.

EMV Chip Acquiring Infrastructure Readiness

Approximately 90% of the existing POS machines are enabled to accept EMV chip cards. The POS terminals are managed by 21 acquirers (APPENDIX H), with 3 acquirers (Axis / HDFC / ICICI) dominating with over 85% market share.

ATMs are currently not enabled for acceptance of EMV chip cards. However, approximately 50% of the existing ATMs are capable with upgrades to hardware and software. The rest 50% of the ATMs need major hardware upgrade (or even replacements) to enable chip card acceptance.

Large scale infrastructure creation - UIDAI

The Unique identification project (UID) is an ambitious project which aims to provide a unique biometric ID for all Indian residents. How this becomes relevant to the working group's consideration is when we consider using the biometric ID as a second factor for authentication of all Card Present transactions. This will require an upgrade of the acquiring infrastructure with Finger print readers.

Some key considerations:

While debit cards account for nearly 90% of the total plastics issued in the country, debit spends are less than 30% of overall spends though growing very fast.

Bulk of the international spends are on Credit Cards

The UIDAI's Aadhaar and its possible ubiquity is a consideration which requires further review pending adoption and usage of UID

Strengthening the Existing Payments Infrastructure

The current payments infrastructure in India requires certain enhancements to make the payment infrastructure secure. These enhancements include:

1. Securing the Technology Infrastructure
    1a. Unique Key per Terminal (UKPT) or Derived Unique Key per Transaction (DUKPT)
    1b. Terminal Line Encryption (TLE)
2. Improving Fraud Risk Management Practices
3. Strengthening Merchant Sourcing and Monitoring Process

1. Securing the technology Infrastructure

Currently all transaction data travels from POS terminal/ATM to the host system in clear text format except for the PIN data. The transaction data travels through various communication carriers like PSTN, IP WAN, GPRS, and CDMA. Any data compromise due to wire-tapping at merchant establishments or during the communication carriage can lead to fraud losses and reputation risk for the issuing and acquiring banks.

The working group deliberated at length on the various solutions that can secure the payment infrastructure. The following 3 solutions are proposed for securing the technology infrastructure:

1a. Unique Key per Terminal (UKPT)

Unique Key per Terminal (UKPT) is a key management scheme, where each POS terminal/ ATM has a unique key for encrypting data originating from a terminal/ATM. UKTP is the common method of encryption implemented worldwide on ATM/POS.

Currently, acquirers in India use a single key to encrypt transaction data originating from all their POS terminals. There is a risk in having the same key across all POS terminals. Incase of key compromise of a particular terminal, then all the terminals of the acquirer are compromised.

Looking at the current practice in the Indian market for POS, the data exposure risk which exists currently, UKPT needs to be adopted.

Derived Unique Key per Transaction (DUKPT)

DUKPT is one level higher form of POS transaction data encryption than UKPT. DUKPT uses one time keys that are generated for every transaction and then the key is discarded. The advantage is that if one of these keys is compromised, only one transaction will be compromised.

1b. Terminal Line Encryption (TLE)

It is critical to build adequate controls to safeguard customer and transaction information during the transaction life cycle. Currently information flow between the acquiring host, issuer host and switch are encrypted; the residual risk being the fact that the transaction data packets flow in clear between the terminal and the acquiring host. This exposes the payment infrastructure to possible data compromise through wire tapping.

TLE also protects against other threats like eavesdropping/card skimming, host spoofing, replay attacks in addition to wire tapping.

TLE offers an encrypted terminal line from the POS terminal to the bank acquirer host when transferring transaction data packets during online transaction processing. It uses a 'Line Encryption Server' which facilitates the encryption and decryption of the transaction data packets.

Many countries across the globe have implemented TLE to secure the payment infrastructure; examples are Malaysia, Thailand, Indonesia, Europe, and USA.

2. Improving Fraud Risk Management Practices

Adoption of appropriate Risk Mitigation Techniques & Strategies

Risk mitigation processes and policies are an integral part of any business strategy; hence it is imperative that adequate risk mitigation strategies and controls are adopted by organizations.

It is important for organizations to have a well defined process of risk management viz. Identification, Detection, Investigation, Deterrence and Prevention. Risk management would encompass all risk types viz Fraud, Credit, Operational, Reputational.

Please refer Appendix D for detailed tabling of Minimum Control Measures (Standards) to be adopted by issuers/acquirers. Also enclosed are certain additional Best Practices which banks could consider. This addresses the below risks:

a. Issuance Risk

b. Merchant Acquiring Risk

c. ATM Risk

3. Strengthening Merchant Sourcing and Monitoring Process

As we strengthen various elements of the payment eco-system, the merchant sourcing process – merchant validation, and monitoring - becomes a weak link/point of failure for the overall system. Hence, there is a need to tighten the current merchant sourcing documentation through the following:

3a. Merchant Sourcing Documentation

The following is the minimum document requirements for sourcing merchants to be followed by acquiring banks. Any exception to the above shall be made by the authorized bank /acquirer.

Merchant Eligibility

1. Merchant Application Form duly signed and stamped by the authorised signatory

2. Merchant Establishment Agreement duly signed and stamped by the authorised signatory.

3. Business License / Registration copy (any of the following)

   - Central / State Sales Tax registration,
   - Municipal Corporation registration,
   - Other Government Registration (e.g. Issued under Shops and Establishments Act, etc.)
   - Certified IT Return or Certified Advance Tax Challan or Certified Professional Tax return
   - Application form for a Govt. License acknowledged by the authority containing merchant name and address and a Receipt of payment to authority
   - Relationship with any other acquirer of greater than 12 months (confirmed by the following two documents - one statement of greater than 12 months and the other not earlier than the previous two months at the time of enrollment)
   - For new establishment where CST / ST number is not available, 'applied for' document will be acceptable

   CST / ST number may be waived for applications from the following establishments:

   i) Central or State Government undertakings viz (Railways, airways, govt emporiums, govt hospitals, customs).

   ii) Schools and Colleges: For these a letter from the authorized signatory on the letterhead will be acceptable.

   iii) Private Hospitals, clinics, diagnostic centers: In these cases a letter from the authorized signatory on the letterhead or relevant registration document copy

   iv) Chemists: For these cases copy of drug license will be acceptable.

In the above document, the Merchant Name and Address to be the same as per the Account Opening Documents (AOD).

v) In case of petroleum merchants, a copy of the agreement with the petroleum company or a delivery challan would suffice)

vi) IATA certification for Travel agents

Note: If the business license has expired and the expiry is less than 3 month from date of sourcing of the ME application, visitation from the local credit officer / Relationship Manager along-with a copy of the expired business license would suffice; else the acknowledgement copy for renewal of license is mandatory.

4. Vintage --Can differ from bank to bank basis individual bank policy.

5. Turnover Criteria -- Can differ from bank to bank basis individual bank policy.

6. Contact Point Verification will be mandatory

7. Merchant negative database check using CIBIL bureau - only post CIBIL infra goes live with merchant repository

8. Signature verification of the authorized signatory (Any of driving license, passport copy, banker's verification, PAN card, Credit Card, others as per the Bank's policy)

9. In addition to above, further documentation as per merchants registered entity type will be required:

   8.1 Partnership
   - Partnership Authority Letter
   - Partnership Deed

   9.2 Hindu Undivided Family (HUF)
   -Declaration by all member of the HUF

   8.3 Private/Public Limited Company
   - Board Resolution
   - Certificate of Incorporation
   - Memorandum of Association
   - Articles of Association

Strengthening the plastic and introducing Second Factor Authentication

Based on detailed evaluation of various options on parameters like customer impact, issuer impact, acquirer impact, merchant impact, global interoperability and residual risks, the following three solutions sets emerge:

1. Magnetic Stripe Card and PIN
2. Magnetic Stripe Card and Biometric (Aadhaar finger print)
3. EMV Chip Card and PIN

1. Magnetic Stripe Card and PIN

Over 99% of the credit and debit cards issued in the country are Magnetic Stripe Cards. Currently, PIN is required only for ATM transactions and not for POS transactions. PIN protects against lost and stolen card fraud.

PIN is prompted on the POS terminal based on the following:

- Service code that is coded in the magnetic stripe of the card at the time of issuing the card or
- BIN (Bank Identification number – first 6 digits of the card number) that is updated on the POS terminal or
- Combination of both service code and BIN.

If Magnetic Stripe Card and PIN is to be mandated for all POS transactions, then:

- Terminals will have to be modified to read the full service code on the card and prompt for PIN
- If the service code on the card does not support PIN prompt, then terminals will have to be updated BINs of all the issuing banks in India This has to be done by updating the application software loaded on the POS terminal.

Magnetic Stripe Card and PIN fulfills the short term objective (next 2/3 years) of protecting against lost and stolen card frauds.

Securing the payment infrastructure is critical prior to the roll out of this option. The effort involved in changing the eco-system is estimated to be 12- 18 months for a complete roll out. MSD+PIN could be a short term solution till such time the industry migrates to a well established long term solution.

2. EMV Chip Card and PIN

EMV Chip Card protects against counterfeit (skimming) card fraud. EMV Chip Card and PIN protects against both counterfeit (skimming) and lost & stolen card fraud.

Currently, only few large issuing banks like Citibank, ICICI Bank, HDFC Bank and SBI are issuing EMV chip cards. Most of other banks' host systems are not ready and are not certified for issuance of chip card. Changes are required on the authorization switch, issuing host, and card embossing platforms.

Banks who are currently issuing EMV Chip cards are issuing as Chip and Signature. None of the issuing banks have started issuing Chip and Pin Cards. Hence, all banks need to make necessary technology changes and get themselves certified to issue Chip and PIN cards.

Based on international experience, EMV Chip Card and PIN migration typically takes 5 years. However, the migration timelines depend on the market size.

Refer Appendix G for more details on EMV Chip and PIN

3. Magnetic Stripe and Biometric (Aadhaar finger print) Authentication

Magnetic Stripe Card and Biometric (Aadhaar finger print) protect against both domestic counterfeit (skimming) and lost & stolen card fraud.
Biometric (finger print) captured by UIDAI can be used as authentication for protection against both domestic counterfeit and lost & stolen card fraud as the cardholder has to be physically be present at the POS terminal/ATM to authenticate the transaction. Even if the card is counterfeited, the fraudster will not be able to use the card as biometric of the customer would be required.

Aadhaar authentication using biometrics provides a strong "Who you are" factor of authentication. This can be combined with a second "What you have" or "What you know" factor to achieve strong customer identification at the point of sale.

This option is technically quite strong. However, acceptance of biometric for payment authentication is not been proven.

Refer Appendix F for more details on Aadhaar and UIDAI

A brief comparison of the above 3 solution options is enclosed in APPENDIX E.

At few merchant categories like fuel stations and restaurants, there are execution challenges in adopting PIN or biometric as additional factor of authentication.

Of all the available options that provides worldwide acceptance but the major disadvantage is in terms of cost of the card and need of reissuance due to short validity of the cards which comes to every 5 years (which is currently 7 to 10 years for debit cards)

Solution Considerations

The following is basis for the recommendations proposed by the Working Group:

1. FRAUD LEVELS

1.1 Fraud to Sales ratios and absolute fraud levels are low as of date, however future proofing payment eco-system is a key consideration.

1.2 Fraud levels on international transactions are significantly higher when compared to domestic transactions.

2. GLOBAL LEARNINGS

2.1 EMV Chip Card is the internationally accepted solution for strengthening authentication of card present transactions. It is also the most widely deployed solution. This is the recommended standard for protecting against skimming by all Payments Associations worldwide.

3. COST

3.1 The cost of EMV Chip Card & PIN solution is quite high relative to the cost of other options and relative to the revenue of the industry.

4. INFRASTRUCTURE READINESS

4.1 Over 90% of domestic acquiring POS infrastructure is EMV Chip Card enabled. However, ATM infrastructure is not enabled for EMV Chip Card.

4.2 Number of debit cards are quite large relative to number of credit cards. Also, there is difference in activation levels at POS. Hence, the need for differentiated approach for debit and credit cards.

5. INDIAN CONTEXT

5.1 India is the only country to have a concept of a biometric (Aadhaar finger print). While it is very early to assess UID for off-take and transaction authentication, UID could be a national asset which, if executed well, will benefit all stakeholders.

5.2 For Domestic transactions, EMV + PIN and Magnetic Stripe + Biometric will achieve similar security goals for protecting against counterfeit and loss and stolen card frauds since UID as additional factor authentication requires the person to be present at the POS terminal at the time of transaction for biometric capture.

In Summary

The working group arrived at the final recommendations based on the following critical factors:

1. Putting in place a series of measures to strengthen the Payments infrastructure and ecosystem in the country
2. The need for a hybrid approach - the evolving nature of UIDAI, varying international and domestic trends.
3. The need for a PIN (to ensure Lost and Stolen fraud is minimized) over and above protecting for skimming (Counterfeit). The choice of PIN though would be at the discretion of the Issuer.
4. Important to ensure that both offline and online PINs are accepted by the EDC machines so that interoperability is ensured.
5. Open, reloadable prepaid cards to be treated as “debit “ equivalent as far as group recommendations as concerned.
6. Differentiated implementation timelines for debit and credit cards.
7. EMV Cards for international travelers to be prioritized
8. Minimize throw-away costs and technology efforts for all stakeholders.
9. Evaluation of UIDAI’s Aadhaar roll out as a strong alternative for domestic transactions 18 months from now based on:
    a. Aadhaar enrollment statistics for the existing cardholder base
    b. Proof of Aadhaar working as a second factor through pilots and roll outs
    c. Readiness of UIDAI to work with ATM, POS and device manufacturers to ensure ubiquity of biometric authentication both for existing machines and new deployments
    d. End to end transaction time including biometric authentication to comply with global standards for authentication
    e. Legal framework to be in place for ensuring non-repudiation of biometric authenticated transactions.
    f. Procedural guidelines and engagement model for banks to work with UIDAI for authentication, validation process in case of dispute through logs etc. to be put in place.
    g. UIDAI’s readiness to work with banks, associations and technology partners to make the payments ecosystem ready for a well tested, industry grade solution 18 months from now
    h. Evaluate the risk of being a ‘single point of failure’

Recommendations

The following are the recommendations of the Working Group:

1. ***Strengthening the existing Payment Infrastructure & Future Proofing the system***

   The first step prior to implementing additional controls and authentication would be strengthening the existing payment infrastructure by securing the technology infrastructure, improving fraud risk management practices across all stakeholders, and strengthening merchant sourcing process. Towards this, the following would be important technical and process changes for the industry to make over the next 24 months:

S. No.	Actionable	Implementation Timelines
Improving the basic infrastructure		
1	All acquirers and issuers may put in place adequate fraud risk management systems and processes	12 months
2	All acquirers to adhere to the merchant sourcing norms envisaged in the report	12 months
3	All acquirers may implement UKPT / TLE	12 / 24 months
Future Proofing the System		
4	Acquiring infrastructure should be commercially ready to accept PIN for transactions. POS Infrastructure to also support EMV Chip Card reading	24 months
5	Issuers to ensure EMV readiness from a technology perspective	24 months
6	In case UID based biometrics is adopted as the second factor, then the acquiring infrastructure (ATM & POS) should be enhanced to accept Biometrics	36 months
7	Ongoing monitoring of fraud trends	To commence right away

2. ***Introducing an Additional factor of authentication: Debit Cards.*** *Also includes fully prepaid (Open) Cards*

Debit Cards	Actionable	Implementation timelines
Debit Cards – Domestic		
1	**Aadhaar roll out evaluation:** MSD + Aadhaar Biometric could be considered as an alternative to EMV +PIN if UIDAI is able to meet authentication requirements of card payments at POS and ATM.	Evaluation in 18 months time
2	All debit card transactions to have a PIN as an additional factor of authentication at POS.	Complete in 24 months. *Start date to tie in with acquiring infrastructure readiness to accept PIN*
3	If the decision is not to adopt biometric Aadhaar authentication, then migrate to EMV + PIN. If decision is to adopt biometric Aadhaar based authentication, overall industry implementation timelines is likely to be lesser than EMV roll out timelines. For issuers who migrate to EMV prior to implementation start date, decision to support Aadhaar authentication would be issuer call. Overall industry migration timelines to be ascertained as part of the Aadhaar evaluation.	EMV +PIN: Roll out to commence in 36 months and to be completed within 4 years from there on. MSD+Aadhaar: *Start date to tie in with acquiring infrastructure readiness to accept biometric authentication and to commence by 36 months*
Debit Cards – International		
4	EMV Chip Card & PIN to be issued when at least one purchase is evidenced on their card in a foreign location	24 months

3.

4. *Introducing an Additional factor of authentication: Credit Cards*

Credit Cards	Actionable	Implementation timelines
Credit Cards – Domestic		
1	**Aadhaar roll out evaluation:** MSD + UID-Aadhaar Biometric to be evaluated as an alternative to EMV+PIN, if UIDAI is able to meet authentication requirements of card payments at POS and ATM.	Evaluation in 18 months time
2	If the decision is not to adopt biometric Aadhaar based authentication, then migrate to EMV + PIN: If decision is to adopt biometric Aadhaar based authentication, overall industry implementation timelines is likely to be lesser than EMV roll out timelines. Overall industry migration timelines to be determined at the time of Aadhaar evaluation. For issuers who migrate to EMV prior to implementation start date, decision to support Aadhaar authentication would be issuer call.	• EMV Chip Card and PIN to be issued to all new and renewal card customers by beginning of year 3. • 70% of all cards to move to EMV Chip Card & PIN by end of year 4 • 100% of cards to move to EMV Chip Card & PIN by end of year 5 MSD+Aadhaar: *Start date to tie in with acquiring infrastructure readiness to accept biometric authentication and to commence by 36 months*.
Credit Cards – International		
4	EMV Chip Card and PIN to be issued to customers who have evidenced atleast one purchase using their card in a foreign location	24 months

IMPORTANT: Based on fraud trends, the migration timeline / approach might vary

Some emerging Technologies to consider in the long run

One of the options available for payment ecosystem players to consider is Contactless smart cards . This of course will come about once the acquiring and the issuing ecosystem evolves and stakeholders start seeing the merit and the commercial viability in investing in a technology like this.

Transit payments (metro rail, buses, toll), Loyalty applications and Micro-transactions might accelerate the move to contactless cards in India. Contactless transactions are known to be significantly faster and more efficient than magnetic stripe / contact cards.

Multiple applications -- ID, access control, debit, credit, transit, toll, e-purse, e-governance could all be based on such contactless cards. There could be varied uses for this e.g. allowing micro-transactions (up to say Rs 1000) to be executed without a PIN

According to Juniper Research, by 2013, one in five smart phones in the world would have Near Field Communication (NFC) capability. NFC is also available as a Micro SD card /sticker. Once the acquiring infrastructure and ecosystem is built for contactless, the same could be seamlessly migrated to NFC.

In India, we could have contactless cards for a large section of the population which cannot afford an NFC phone. The others might migrate to the cardless convenience of the NFC phone.

END OF REPORT

Appendix A – Industry Size

Data Points		Figures (Count in Numbers, Value in INR)	Source
Number of POS Terminals		5,65,542	RBI
Number of ATMs		70,462	RBI
Number of cards	– Credit	1.8 Crores	RBI
	– Debit	22.2 Crores	
Credit Cards : POS* Transactions	– Value	75,328 Crores	RBI
	– Count	26 Crores	(Mar 2010 – Feb 2011)
ATM Transactions	– Value	1,061 Crores	
	– Count	0.2 Crores	
Debit Cards : POS* Transactions	– Value	37,760 Crores	RBI
	– Count	23 Crores	(Feb 2010 – Feb 2011)
ATM Transactions	– Value	10,90,053 Crores	
	– Count	415 Crores	

Industry Data : Credit Cards (Domestic, International & Net of Ecommerce)			
Data Points		**Figures (Count in Numbers, Value in INR)**	**Source (Classification Derived From)**
POS* Transactions Value	– Domestic	70,808 Crores	Visa : Domestic - 94%
	– International	4,520 Crores	Int'l - 6%
Count	– Domestic	25 Crores	Visa : Domestic - 98%
	– International	0.5 Crores	Int'l - 2%
POS Only Transactions Value (Net Ecommerce)			(Net Ecommerce)
	– Domestic	53,814 Crores	Visa : Domestic - 76%
	– International	2,305 Crores	Int'l - 51%
Count (Net Ecommerce)			(Net Ecommerce)
	– Domestic	18.3 Crores	Visa : Domestic - 72%
	– International	0.2 Crores	Int'l - 36%
ATM Transactions Value	– Domestic	934 Crores	MasterCard : Domestic - 88%
	– International	127 Crores	Int'l - 12%
Count	– Domestic	0.19 Crores	MasterCard : Domestic - 93%
	– International	0.01 Crores	Int'l - 7%

Industry Data : Debit Cards (Domestic, International & Net of Ecommerce)			
Data Points		**Figures (Count in Numbers, Value in INR)**	**Source (Classification Derived From)**
POS* Transactions Value	– Domestic	36,627 Crores	Visa : Domestic - 97%
	– International	1,133 Crores	Int'l - 3%
Count	– Domestic	22.8 Crores	Visa : Domestic - 99%
	– International	0.2 Crores	Int'l - 1%
POS Only Transactions Value (Net Ecommerce)			(Net of Ecommerce)
	– Domestic	32,598 Crores	Visa : Domestic - 89%
	– International	691 Crores	Int'l - 61%
Count (Net Ecommerce)			(Net of Ecommerce)
	– Domestic	20.7 Crores	Visa : Domestic - 91%
	– International	0.2 Crores	Int'l - 68%
ATM Transactions Value	– Domestic	9,48,346 Crores	MasterCard : Domestic - 87%
	– International	1,41,707 Crores	Int'l - 13%
Count	– Domestic	398.4 Crores	MasterCard : Domestic - 96%
	– International	16.6 Crores	Int'l - 4%

POS* - includes POS / E Com / IVR / MOTO transactions

Appendix A (Continued)

Fraud Type	Credit (INR Crores)	Debit (INR Crores)	Total (INR Crores)	Source
Counterfeit & Lost & Stolen (POS)	12.01	1.18	13.19	Visa/MasterCard
MOTO/CNP	22.88	0.21	23.09	Visa/MasterCard
Others	4.11	0.01	4.11	Visa/MasterCard
Total	**39.00**	**1.40**	**40.40**	
Spends Value (Net ATM)	74,079	36,897	1,10,976	RBI Data**
Fraud to Spends Ratio (in bps) (Total Fraud Net ATM)	**5.26**	**0.38**	**3.64**	
POS Spends Value (Net of Ecommerce & ATM)	55,189	32,529	87,717	RBI Data**
Fraud to Spends Ratio (in bps) (POS Only Net Ecom & ATM)	**2.18**	**0.36**	**1.50**	
**Note: Transaction volumes for 12 months considered for calculation				

Credit Cards Fraud Data (POS Only)			
Fraud Type	**Credit (INR Crores)**	**Domestic (INR Crores)**	**Int'l (INR Crores)**
Counterfeit & Lost & Stolen (POS)	12.01	5.60	6.41
MOTO/CNP	22.88	11.26	11.26
Others	4.11	3.38	0.72
Total	**39.00**	**20.24**	**18.76**
Spends Value (Net ATM)	74,079	69,634	4,445
Fraud to Spends Ratio (bps) (Total Fraud Net ATM)	**5.26**	**2.91**	**42.21**
POS Spends Value (Net of Ecommerce & ATM)	55,189	52,922	2,267
Fraud to Spends Ratio (bps) (POS Only Net Ecom & ATM)	**2.18**	**1.06**	**28.28**

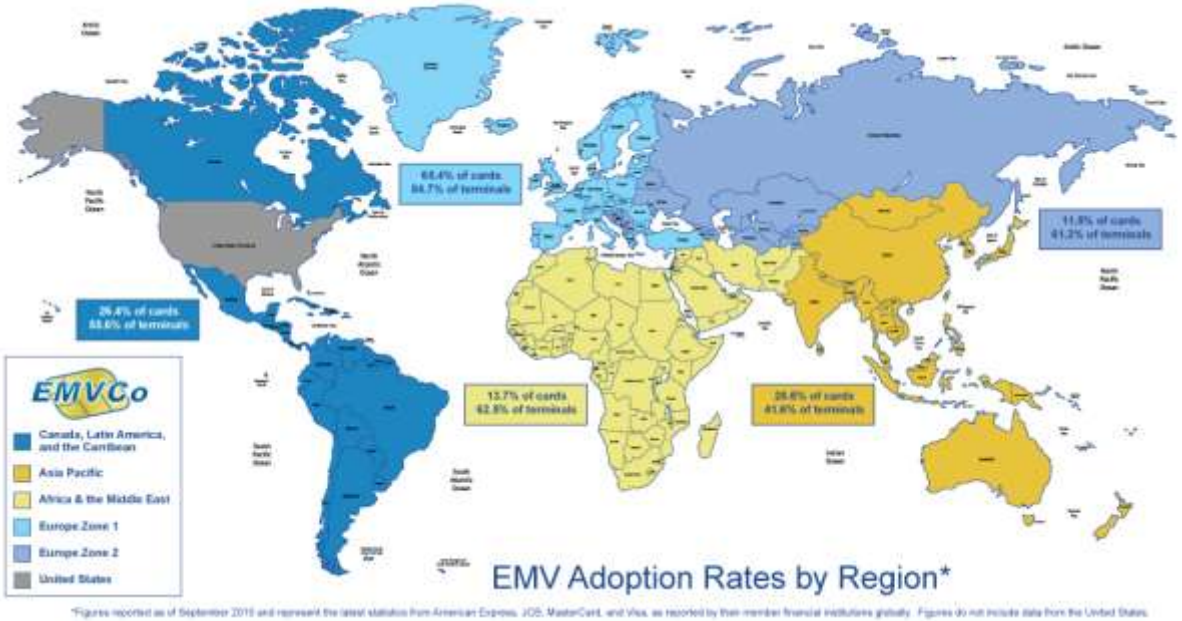
Debit Cards Fraud Data (POS Only)			
Fraud Type	**Credit (INR Crores)**	**Domestic (INR Crores)**	**Int'l (INR Crores)**
Counterfeit & Lost & Stolen (POS)	1.18	0.61	0.57
MOTO/CNP	0.21	0.07	0.14
Others	0.01	0.01	--
Total	**1.40**	**0.69**	**0.17**
Spends Value (Net ATM)	36,897	35,790	1,107
Fraud to Spends Ratio (bps) (Total Fraud Net ATM)	**0.38**	**0.19**	**6.41**
POS Spends Value (Net Ecommerce & ATM)	32,529	31,853	675
Fraud to Spends Ratio (bps) (POS Only; Net Ecom & ATM)	**0.36**	**0.19**	**8.44**

Appendix B - EMV Worldwide Deployment & Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Caribbean	182,185,043	26.4%	2,000,000	55.6%
Asia Pacific	305,126,927	26.6%	3,200,000	41.6%
Africa & the Middle East	16,841,874	13.7%	348,000	62.5%
Europe Zone 1	555,688,434	65.4%	9,400,000	84.7%
Europe Zone 2	22,817,271	11.5%	457,800	61.2%
United States^				
Totals	**1,082,659,549**	**36.0%**	**15,405,800**	**65%**

* Above figures reported in September 2010 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

^Figures do not include data from the United States.



Appendix C - Stress Test Inferences and Global EMV Migration Experiences

1 Stress Test Inferences

The working committee studied the fraud trends across other geographies and conducted stress test by extrapolating the fraud exposure and ratios basis the trends noticed in other countries. The inferences drawn basis the stress tests conducted are listed below for reference:

- In the absence of 2FA for POS transactions there is a possibility of the fraud losses increasing by more than 200% in a single year in the event of a sharp increase in fraud incidents in the country.
- There is also possibility of POS FTS (Fraud to Sales ratio) increasing by around 200 basis points in one year under adverse conditions.
- Once EMV Chip migration is done, the fraud migrates to other fraud types as listed below
    - Increase in card not present frauds.
    - Increase in frauds on account of fall back transactions
    - Increase in international counterfeit (usage mostly in non EMV markets)
    - Increase in Lost/ Stolen frauds in case Chip + Signature is implemented.

Inferences drawn from these case studies clearly indicate the need to have a much stronger authentication mechanism and reiterate the need for a Second factor for Card Present Transactions. More importantly the case studies also indicate the need to start working towards implementation of Second factor immediately, to be ready to combat frauds in case adverse conditions arise. Even if EMV Chip is adopted by issuers, the need to have adequate control over fall back transactions and second factor in form of PIN is reiterated basis global experience and the stress test and case studies.

2 European payment card industry experience on Chip and PIN migration

There is a clear consensus that the migration to Chip and PIN is bringing significant benefits to the European payment card industry. Indeed, the implementation of Chip and PIN is seen as significant for several reasons:

- **Security**

In those countries with a mature Chip and PIN acceptance environment, the technology has contributed to a marked decrease in fraud from counterfeit and lost and stolen cards – which traditionally accounted for the majority of losses.

As addressed throughout the document, however, there has been a definite migration to card-not-present (CNP) fraud losses and an increase in cross-border counterfeit fraud, particularly at ATMs.

Chip and PIN has contributed to a marked decrease in fraud from counterfeit and lost and stolen cards

- **Capability**

As well as delivering increased security, Chip technology is enabling banks and merchants alike to extend the reach of cashless payments.

For example, contactless payments are seen as a natural “add on” to EMV. Similarly, Chip and PIN is enabling a big increase in unattended or self-service payments.

EMV Chip technology enables banks and merchants to extend the reach of cashless payments. It has facilitated a big increase in unattended or self-service payments

- **A smooth and effective migration process**

In each of the three countries investigated in this document, the migration from signature to PIN has been smooth and effective.

Consumers and merchants alike have been quick to adapt to the new Cardholder Verification Method (CVM). Acceptance issues (whereby, for example, a retailer refuses to accept a magnetic stripe card or a signature-preferring Chip card) have been minimal, and there has been no negative impact on the volume of card payments. On the contrary, it has been suggested that the change may have contributed to a progressive increase in POS spending volume.

Acceptance issues have been minimal

- **Positive reactions to the change**

Reactions from all stakeholders have generally been very positive. When the European payment card industry planned the migration to EMV, it initially considered a Chip and signature solution. However, it was soon acknowledged that this would have limited benefits to merchants, and the retail community was extremely resistant.

By contrast, the retail community became a strong advocate of Chip and PIN. In the UK in particular, large retail groups have cited:

• Quicker checkout times

• Reduced administration costs

• Lower fraud rates

• Fewer chargebacks

Also, many merchants have been quick to deploy additional card payment facilities (which are either enabled by, or made far more secure by Chip and PIN). This includes self-checkout facilities, and other types of self-service payment (such as unattended transport ticketing, vending and pay-at-pump fuel payments).

All evidence suggests that consumers have reacted equally positively. They have adapted quickly to the change and see that it delivers increased security.

Similarly, a traditionally hostile media has generally reacted positively to the change, portraying it as a logical and positive step forward by the payment card industry.

Merchants have been quick to deploy additional card payment facilities

Cardholders have adapted quickly to Chip and PIN at POS and see that it delivers increased security

- **Important lessons learnt**

Although the change has been smooth and effective, the European payment card industry acknowledges that important lessons have been learnt:

1. **The migration of fraud**

To derive maximum benefit from Chip and PIN, issuers and acquirers alike need to be aware of the way fraud migrates, and be prepared to implement new risk management disciplines. Particular consideration needs to be given to those acceptance environments that are yet to be Chip and PIN-enabled.

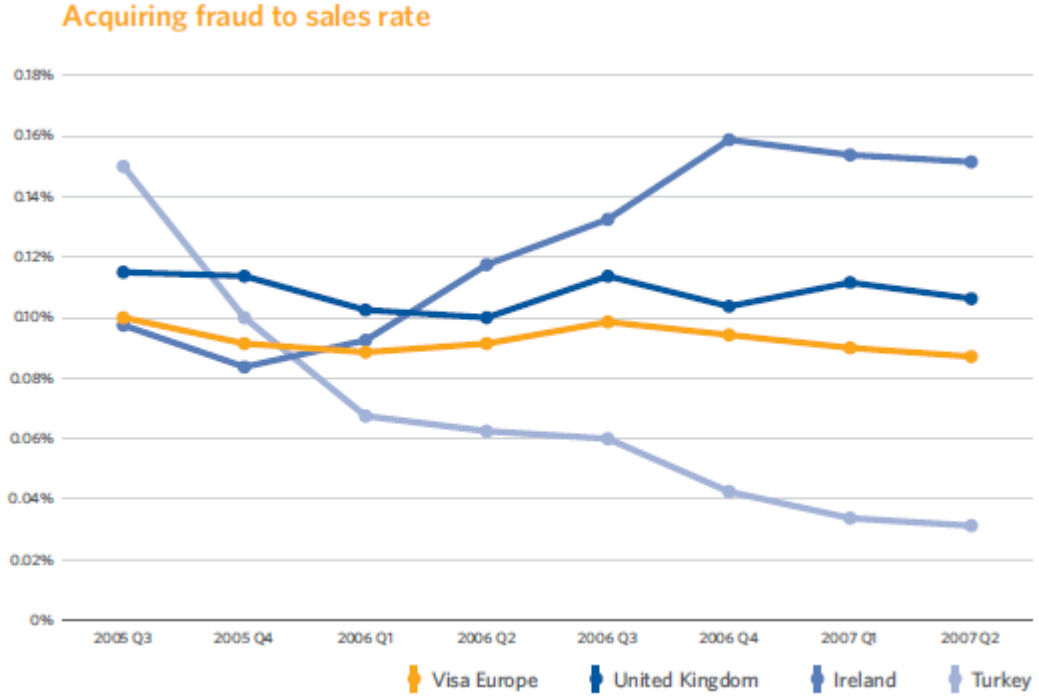
2. **PIN integrity considerations**

As the use of PIN becomes more commonplace, issuers and acquirers alike need to be aware of the risks of PIN compromise and take measures to ensure that any such risks are minimised (through, for example, a programme of cardholder and merchant education/communication).

3. ATM security considerations

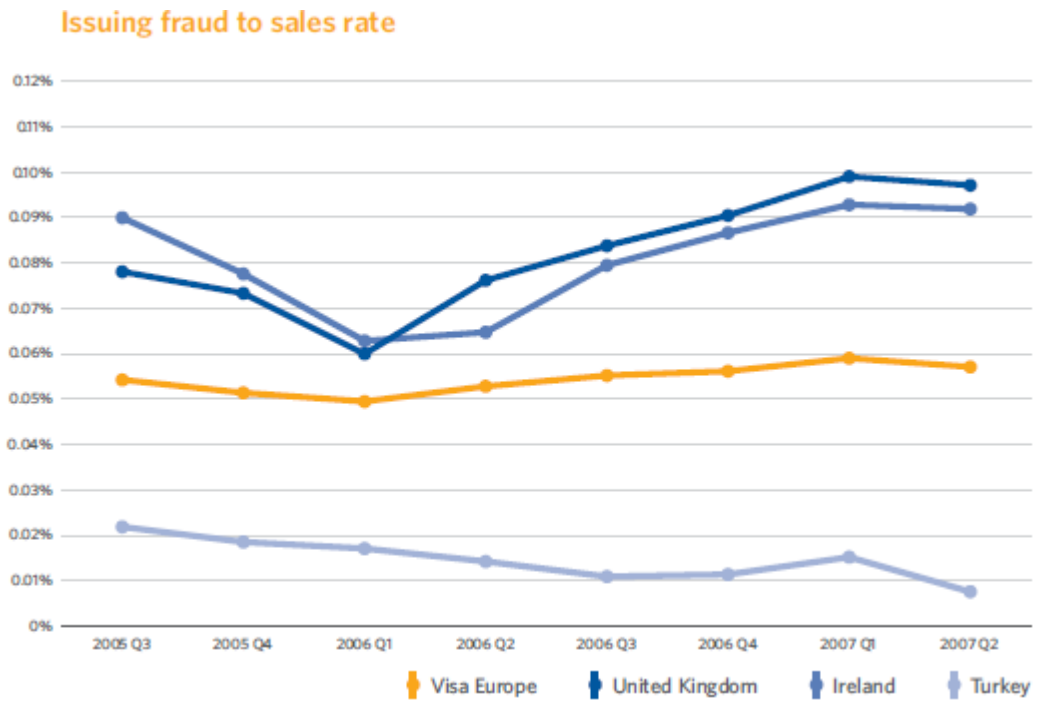
Banks need to treat their domestic ATM estates as an absolute priority (quickly upgrading them to EMV and ensuring that effective anti-skimming measures are implemented). Also issuers need to put new risk management measures in place to identify and avoid the risks of fraudulent ATM withdrawals (such as new authorisation parameters and also anti-counterfeit tools such as iCVV).

We have reviewed the Post migration experiences of select European Countries that have implemented EMV Chip + PIN and the results are as below



Source – Visa Europe

In terms of acquired fraud, a broadly similar pattern can be seen in all three countries. Thanks to chip and PIN, acquirers have been able to stabilise and, in many cases, reduce fraud losses in those instances where the card is present. For CNP transactions, however, acquirers have seen a marked increase in losses.



Source – Visa Europe

In terms of issued fraud, a similar picture emerges across all three countries. Domestic card-present fraud losses have seen a significant reduction. However, savings have been offset by increases in cross-border counterfeit and CNP fraud.

Appendix D – Merchant Sourcing and Monitoring

Minimum Control Measures (Standards) and Additional best practices

Issuer Risk Mitigation

Every financial institution or organization which is in the business of issuance of cards (Credit Cards, Debit Cards, Prepaid Cards) need to ensure adherence to the following Minimum Control Standards. Wherever the activities are outsourced, the respective issuers would still be responsible for ensuring adherence to the standards.

Minimum Control Measures (Standards)

No	Process / Policy
1	Policy which details the risk mitigation strategies and fraud control processes and procedures adopted by the organization
2	Fraud mitigation strategies including all aspects of fraud control viz Detection, Investigation, Deterrence & Prevention and would include the following: • Fraud Detection Capability • Transaction Monitoring • Online SMS Alerts • Investigation capability • Reporting of Frauds to regulators, franchisee and senior management
3	Fraud Trends to be reviewed by Senior Management including Board of directors at least once in a Quarter and board to be informed of any significant frauds or alarming trends.
4	Adequate due diligence to be exercised prior to outsourcing activities to Third party service providers or vendors
5	Maintain database of negative profiles including applicants, customers, vendors etc and ensure that de-dupe is done against this base prior to enrolment.
6	Adequate Data security measures and controls in place in line with industry standards (PCIDSS) and standards prescribed by franchisee and RBI from time to time
7	Customer Education on Emerging Fraud trends and Dos and Don’ts at regular frequency – minimum at least once in a quarter.

Additional Best Practices which could be considered by banks to enhance controls

No	Process / Policy
1	Implementation of Fraud Detection Systems and Authorization Systems with Real time intervention capability
2	Sharing of Negative data base at an industry level
3	Detection basis monitoring of customer authentication transactions i.e. monitoring of static data changes, monitoring of IP address etc
4	Adequate controls over static data changes like mobile number changes etc

Merchant Acquiring Risk Mitigation

Minimum Control Standards – Acquiring Risk

All Acquirers in the business of merchant acquiring need to ensure adherence to the Minimum Control Standards.

Wherever the activities are outsourced, the respective acquiring banks would still be responsible for ensuring adherence to the standards.

No	Process / Policy
1	Merchant Acquiring Policy document which is signed off by senior management team and is approved by the Board.
2	Adequate due diligence including site visits and evaluation at the time of enrolment of merchant. This would include adequate verification of background of merchants and fulfillment of KYC norms.
3	Merchant Training process
4	Monitoring of merchant transactions and settlement trends and capability of investigate suspicious or out of pattern trends. Periodic review and monitoring of merchants
5	Fraud mitigation strategies including all aspects of fraud control viz Detection, Investigation, Deterrence & Prevention and would include the following: • Fraud Detection Capability • Transaction & Settlement Monitoring • Investigation capability Reporting of Frauds to regulators, franchisee and senior management
6	Fraud Trends to be reviewed by Senior Management including Board of directors at least once in a Quarter
7	Authorization Code Validation process (This process would ensure that authorization codes are validated and any mismatch to be investigated by the acquirer)

8	Adequate control over Key entry / off line transactions and merchants. Such facilities should be provided to merchants who have specific requirement only and the same should be approved by Senior management team and transactions from these merchants should be tracked closely
9	Creation of an industry Negative Database for merchants
10	Adequate due diligence to be exercised prior to outsourcing activities to Third party service providers or vendors
11	Adequate Data security measures and controls in place in line with industry standards (PCIDSS) and standards prescribed by franchisee and RBI from time to time Strengthening the infrastructure – Unique Key per terminal / Terminal line encryption, PCI DSS compliance at merchant level.

Additional Best Practices which could be considered by banks to enhance controls

No	Process / Policy
1	Merchant hold funds process for suspicious transactions (coupled with appropriate clause in merchant agreement and a well laid down process with regard to the same to protect the interests of all stakeholders).
2	Merchant Seeding process.
3	Risk grading for merchants and control measures can be decided basis the Risk grading.
4	Adequate control over static data changes like merchant address, phone numbers etc.

ATM Risk Mitigation

Minimum Control Standards – ATM Risk

Given the recent fraud trends it is imperative that adequate controls are placed to safeguard the ATM infrastructure and enhance security of ATM transactions.

a. The below mentioned processes should be implemented by the issuers with regard to usage of cards for ATM transactions and by the acquirers / outsourced service providers who are involved in the ATM installation and acquiring.

No	Process / Policy
1	Fraud Detection Capability
2	Fraud mitigation strategies including all aspects of fraud control viz Detection, Investigation, Deterrence & Prevention and would include the following: a. Fraud Detection Capability b. Transaction & Settlement Monitoring (Acquiring) c. Online SMS Alerts d. Investigation capability e. Reporting of Frauds to regulators, franchisee and senior management
3	Process for Reporting such transactions to franchisee and regulators • All Frauds to be reported to AMT Payment Networks and RBI ATM Payment Networks could develop various risk mitigation processes / services basis the frauds reported by members which would include the following: • CUP (Common Usage Point) Service (To identify common usage points , concentration of frauds at ATM locations) • Authorization intervention strategy for ATM IDs where frauds are noticed – for e.g. block transactions from a terminal ID where fraud is suspected. • Transaction limits (basis issuer requirements)
4	Creation of Negative Database & sharing of such negative information across industry players. (These could be based on ATM ID, location, Vendors etc)
5	ATM Surveillance (Security Guards, Camera etc)
6	Robust Cash reconciliation process

7	Robust cash handling process and fidelity insurance
8	Adequate due diligence prior to appointment of vendors, security staff and prior to outsourcing of activities to TPPs.
9	Adequate Data security measures and controls in place in line with industry standards (PCIDSS) and standards prescribed by franchisee and RBI from time to time.
10	Regular health checks conducted by physical visits to ATM locations to cross check the infrastructure

** Please note: Above mentioned controls / processes should be adopted in addition to existing controls recommended by RBI like validation of PIN for every transaction at ATM etc.,

Additional Best Practices which could be considered by banks – ATM Risks

No	**Process / Policy**
1	Adoption of technology like Jitter, EMV etc
2	Dynamic PIN for ATM transactions (OTP) – like other best practices would be issuer decision to implement depending on implementation challenges, their respective customer base etc.
3	Database of Negative addresses (high risk locations which are prone to physical attacks, compromise)

Appendix E – Solution Set Comparison

Magnetic Stripe & PIN (Static PIN, Dynamic PIN, Software Token, Hardware Token)	**EMV Chip Card & PIN**	**Magnetic Stripe & Biometric (Aadhaar finger print)**
Pros: 1. PIN protects customers against lost or stolen card fraud	Pros: 1. EMV Chip Card protects customers against counterfeit fraud. 2. EMV Chip Card & PIN protects against both counterfeit and lost or stolen card fraud.	Pros: 1. Protects against both counterfeit and lost or stolen card fraud.
Cons: 1. Does not address counterfeit fraud. 2. Migration of fraud to ATM if the same PIN is used for POS & ATM. 3. Dynamic PIN: Quite cumbersome for POS transactions.	Cons: 1. Magnetic Stripe data of EMV Chip cards can be counterfeited and misused in non-EMV countries.	Cons: 1.Scalability, stability, & adaptability of biometric (Aadhaar finger print) for payment authentication is currently untested. 2. Does not address international counterfeit card fraud and lost or stolen card fraud.
Approximate Cost Estimates: X	**Approximate Cost Estimates: 34X**	**Approximate Cost Estimates: 3X*** * *Aadhaar roll for authentication very nascent. Best effort estimate based on data and inputs currently available*

Appendix F - UIDAI (Unique Identification Authority of India)

The Unique Identification Authority of India (UIDAI), is an agency of the Government of India responsible for implementing the envisioned Multipurpose National Identity Card or Unique Identification card (UID Card) project in India. It was established in February 2009, and will own and operate the Unique Identification Number database. The authority will aim at providing a unique number to all Indians, but not smart cards. The authority would provide a database of residents containing very simple data in biometrics. The brand name of the Unique Identification number (UID) is called as Aadhaar.

The UIDAI's mandate is to issue every resident a unique identification number linked to the resident's demographic and biometric information, which they can use to identify themselves anywhere in India, and to access a host of benefits and services. The number (referred to until now as the 'UID') has been named Aadhaar, which translates into 'foundation', or 'support'. This word is present across most Indian languages and can therefore be used in branding and communication of the UIDAI program across the country.

UIDAI has already issued around 73 lakh Aadhaar numbers and will soon launch its authentication services. The authentication infrastructure is being sized to handle a large volume of authentications that will be generated by Government and other sectors. Aadhaar authentication using biometrics provides a strong “Who you are” factor of authentication. This can be combined with a second “What you have” or “What you know” factor to achieve strong customer identification at the point of sale. ATM and POS infrastructure can be upgraded to include an additional biometric scanner.

UIDAI has also published MicroATM standards, encryption Standards, and biometric standards, which allows for secure interoperable payment transactions based on biometric authentication. In many cases, as has been demonstrated by the financial inclusion projects of various banks, biometric provide an inclusive factor of authentication for a population that finds it hard to use a PIN.

All payment networks: Visa, MasterCard, and NPCI are actively working with UIDAI on laboratory and field pilots. The biometric payload adds up about 500 bytes of additional data to the transaction, which is easily handled by the payments switching architecture. As the systems are tested in a production environment and mature, various Banks have plans to roll out Aadhaar linked payment products. Even at the early stages of UIDAI the working group debated and agreed upon that this is a strong potential future option for country like the size of India can adopt for its payment transaction authentications.

The working committee has considered Biometric (UID) as the second factor in one of the solution sets; however the decision to adopt this would depend on various factors like number of UIDs issued to the population which transacts on cards, error rates, authentication network capability to handle transaction volumes, network capability to handle enhanced transaction size and acquiring infrastructure.

Appendix G - EMV (Euro pay, Master Visa Standards)

The EMV Integrated Circuit Card Specifications for Payment Systems are global payment industry specifications that describe the requirements for interoperability between chip based consumer payment applications and acceptance terminals to enable payment. The specifications are managed by the organization EMV Co.

The EMV standards were started by a working group created in 1993 by the world's three mainstream payment organizations: EUROPAY (EPI), MasterCard (MCI) and Visa. The name EMV is derived from the first letter of each of these three organizations.

Now EMVCo is owned by American Express, JCB, MasterCard and Visa, who manages, maintains and enhances the Integrated Circuit Card (ICC) Specifications to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs. The group's objective is to define a common set of standards (EMV standards) for smart card based payment applications. These standards allow the card and the acceptance device to work seamlessly and securely together.

The EMV specifications were written with the following objectives:

- The card and acceptance device must communicate together and indicate what applications the card and acceptance device have in common.
- The acceptance device can run common applications and ensure that minimum standards for risk control and security are applied for that common application.
- The microprocessor-based payment card provides worldwide acceptance and interoperability.

The EMV specifications provide a set of rules that allow a chip card and the acceptance device to communicate with one another. The EMV specifications are based upon the common set of standards developed by the International Organization for Standardization (ISO) for integrated circuit (chip) cards and related acceptance devices. The current version of the EMV '96 specifications (version 3.1.1), published in May 1998, defines requirements for the interaction of debit and credit card functions on a chip card and a terminal. The components in these specifications cover requirements for cards, applications, and terminals. A new release EMV2000 (EMV 4.2) is currently available.

EMV is designed to significantly improve the security for consumer card payments by providing enabling features for reducing fraudulent payment that results from counterfeit and lost and stolen cards.

The features that are defined by EMV are as follows -:

1. Authentication of the chip card to verify that the card is genuine so as to protect against counterfeit fraud for both online authorized transactions and offline transactions.
2. Risk management parameters to define the conditions under which the issuer will permit the chip card to be used and force transactions online for authorization under certain conditions such as offline limits being exceeded.
3. Digitally signing payment data for transaction integrity.
4. More robust cardholder verification to protect against lost and stolen card fraud for EMV transactions.

In order to accelerate the deployment of EMV technology, existing card schemes have implemented fraud liability shift. These rule changes “shift” liability for fraud that could have been prevented if EMV chip and/or PIN technology had been used, by both parties, to the issuing or acquiring party that had not invested in EMV chip and / or PIN equipment.

EMV supports two different types of data authentication:

Offline Data Authentication: The Offline Data Authentication ensures that the ICC card is not counterfeited and that the data is not deteriorated or falsified. It is a process whereby the card is validated at the point of transaction using RSA public key technology to protect against counterfeit or skimming. The flow of the EMV transaction ensures to authenticate the card and the terminal in the process by means of verifications of the cryptograms. The keys used as part of certificates in the cards as well as the public keys on the terminals is in general 10 years and there are multiple keys active and loaded in terminals at any given point to support all the existing EMV cards in the market.

Online Data Authentication: The Online Data Authentication further ensures the card issuer that the card used in the transaction is actually the card issued by the issuer.

EMV includes three forms of Offline Data Authentication:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA/AC Generation (CDA)

Note: RSA (Rivest, Shamir and Adleman - the inventors of the RSA cryptosystem) public key technology.

Static Data Authentication (SDA):

SDA is a type of Offline Data Authentication whereby the terminal validates a cryptographic value placed on the card during personalization of the card. This validation protects against some types of counterfeit, but does not protect against copying and replaying attack.

Dynamic Data Authentication (DDA):

DDA is a type of Offline Data Authentication where the card generates a digital signature using transaction-specific dynamic data elements, for validation by the terminal to protect against skimming.

Combined DDA/Application Cryptogram Generation (CDA):

CDA is a type of Offline Dynamic Data Authentication, combined with processing of the transaction application cryptogram.

Appendix H – Acquirer wise terminals data

Acquirer Bank Name	# Terminals as on Mar 2011	# EMV Chip Enabled Terminals as on Mar 2011 (of # Terminals)
Andhra Bank	0.36%	3.58%
Axis Bank Limited	31.82%	88.93%
Bank of Baroda	0.85%	99.92%
Bank of India	0.33%	0.00%
Canara Bank	0.11%	0.00%
Central Bank of India	0.13%	0.00%
Citibank, N.A.	1.77%	88.35%
Corporation Bank	2.75%	100.00%
Deutsche Bank AG	0.01%	100.00%
Development Credit Bank Ltd	0.19%	100.00%
HDFC Bank Limited	18.85%	92.42%
ICICI Bank Ltd	35.39%	100.00%
IDBI Bank Ltd.	2.53%	93.32%
Jammu And Kashmir Bank Limited	0.46%	83.90%
Karnataka Bank Limited	0.00%	0.00%
Oriental Bank of Commerce	0.33%	100.00%
Syndicate Bank	0.06%	100.00%
The Federal Bank Ltd	0.31%	100.00%
The HSBC Limited	3.09%	0.00%
Union Bank of India	0.46%	100.00%
Vijaya Bank	0.20%	0.00%
Total	100.00%	90.39%