Regulations for Payment Card Security

PAYMENT SYSTEMS DEPARTMENT

STATE BANK OF PAKISTAN

Acronyms

ADCs	Alternate Delivery Channels
ATM	Automated Teller Machine
BCO 1962	Banking Companies Ordinance, 1962
DRC	Dispute Resolution Center
DRM	Dispute Resolution Management
CSF	Card Security Framework
CVM	Cardholder Verification Method
CSP	Card Service Provider
EMV	Europay Mastercard Visa
FI	Financial Institution
FATF	Financial Action Task Force
FRM	Fraud Resolution Management
FRMU	Fraud Risk Management Unit
IC Card	Integrated Circuit Card
IVR	Interactive Voice Response
NPMs	New Payment Methods
PA DSS	Payment Application Data Security Standard
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standard Council
PIN	Personal Identification Number
POS	Point of Sale
PSD	Payment Systems Department
PS&EFT, 2007	Payment Systems and Electronic Fund Transfers Act, 2007
SBP	State Bank of Pakistan
SMS	Short Message Service
SLAs	Service Level Agreements
SOP	Standard Operating Procedure
STC	Social Transfer Card
TAT	Turn Around Time
TOR	Terms of Reference

Table of Contents

1. Preamble

Payment Systems have significant importance in an economy, as they enable the efficient conduct of trade, commerce and other economic activities. The stability of financial system is derived from the safety, competitiveness and efficiency of the payment channels and corresponding instruments. The use of electronic means of transactions has facilitated the masses in affecting transactions instantly. However, it has its own risks as well, if the security of the channels or the instrument is compromised. In electronic banking, share of Payment Card based transactions has grown significantly in overall banking transactions. With the increased growth in Payment Card transactions, its security has gained importance due to rising threats and vulnerabilities associated with it. State Bank of Pakistan's oversight role of Payments Systems is aimed principally at ensuring that existing systems are safe, resilient, and maintain the confidence of consumers. Thus, SBP, under its objective to promote modern and robust Payment Systems has issued "Regulations for Payment Card Security" that will facilitate the Card Service Providers (CSPs) to develop a Card Security Framework, while aligning their information security objectives with SBP's strategic objectives. Moreover, CSPs are also encouraged to evaluate effectiveness of existing security controls against each threat and vulnerability in the New Payment Methods (NPMs) in the light of guidance provided by global bodies like Financial Action Task Force (FATF).

2. Definitions

1. **Acquirer:** is the entity that holds deposit accounts for card acceptors/ merchants and to which the card acceptors/ merchants transmit the data relating to the transaction. The acquirer is responsible for the collection of transaction information and settlement with the acceptor/ issuer.
2. **Authorised Government Entity:** is an entity authorised by the Federal/ Provincial Government of Pakistan, for managing the operations of a social transfer program.
3. **Bank:** means a scheduled bank as defined in Section 5 of the Banking Companies Ordinance, 1962 or a microfinance bank as defined in Microfinance Institutions Ordinance 2001.
4. **Payment Card:** Any card including an ATM card, debit card, credit card, prepaid card or stored value card, used by a Consumer to affect an electronic transaction
5. **Card Service Provider:** For the purpose of these regulations, CSPs are those entities that fall under SBP's regulatory and supervisory ambit and include but not limited to Commercial Banks, Microfinance Banks, Payment System Operators, Payment Service Providers or any other entity that is in the business of issuing, acquiring and processing Payment Card.
6. **Financial Institution:** Financial Institution as defined in the Financial Institutions (Recovery of Finances) Ordinance, 2001(XLVI of 2001) and includes a banking company or any other Electronic Money Institution or person, authorized by the State Bank in this behalf, that directly or indirectly holds an account belonging to a consumer.
7. **Fraud Resolution:** It is the process of identification, analysis, and resolution of issues pertaining to fraud.
8. **Issuer:** is the bank which issues payment cards (debit/ credit/ prepaid cards etc) to accountholders/ customers.
9. **Payment Scheme:** are a set of interbank rules, practices and standards necessary for the functioning of payment services and may include card schemes comprising technical and commercial arrangements, setups to serve one or more brands of card which provides the organizational, legal and operational framework necessary for the functioning of the services marketed by those brands or internet based E-Commerce schemes.
10. **PA DSS:** It is the global security standard created by the Payment Card Industry Security Standards Council (PCI SSC).
11. **PCI DSS:** PCI DSS is a global data security standard adopted by Payment Card brands that process, store or transmit cardholder data and/or sensitive authentication data.

12. **Security Breach:** Any incident that results in unauthorized access of systems, applications, data, services, networks and/ or devices that bypass their underlying security mechanisms.
13. **Social Transfer Card:** is a prepaid card issued by a Bank under a formal agreement with an authorised government entity for a specific purpose of disbursing funds to assist the underserved segment of the country.
14. **Two Factor Authentication:** A combination of two different factors of authentication among three known factors; something the user knows, something the user has and something the user is.

3. Applicability & Scope

Regulations for Payment Card Security are applicable to all CSPs that are in the business of issuing, acquiring or processing Payment Cards. These Regulations shall cover all types of Payment Cards excluding Social Transfer Cards.

4. Card Security Framework

CSPs shall develop and implement a comprehensive CSF by taking into consideration various types of risks associated with the Payment Cards, their usage patterns and the cardholder profile. The CSF shall define clear roles and responsibilities of Senior Management, Officials responsible for managing Payment Card business and the relevant stakeholders.

The CSF for Payment Cards shall be part of already existing bank wide security framework in order to holistically address security concerns. However, CSPs shall develop a new CSF, if bank wide security framework does not cover CSF. The CSF shall be approved by relevant Board Committee or Senior Management followed by ratification by full Board. Further, the CSF shall be reviewed by the BOD or senior management of the FI, at least once in a year. The CSF, as a minimum, shall be comprised of but not limited to the following:

I. Security Risk Assessment
II. Security Controls Implementation and Monitoring

4.1. Security Risk Assessment

It is the process of identifying, estimating and prioritizing security risks to which organization's assets i.e. consumers, Information Technology and communication resources etc are exposed. CSPs are required to do the following:

a. CSPs shall conduct comprehensive risk assessment and information security review of Payment Card systems and operations.
b. CSPs shall identify and prioritize risks as High, Medium and Low, associated with Payment Card operations.
c. CSPs shall assess potential threats and vulnerabilities in Payment Card related systems.
d. CSPs shall perform an impact assessment to estimate the degree of overall loss that may occur as a result of the exploitation of Payment Card security vulnerability.
e. CSPs shall perform assessment to estimate the probability of occurring threat and determine the circumstances that shall affect the likelihood of the risk occurrence.
f. In case of international usage of Payment Cards, the risk assessment shall commensurate with the risks of cross border usage.
g. CSPs shall carry out an immediate risk assessment, when there is a security breach to Payment Card system, significant changes to the infrastructure and an introduction of a

new product or service. In case of a Security Breach, a detailed report shall be submitted to PSD, SBP within a fortnight of occurrence as per the format at "*Annexure A: Card Security Data Breach Report*" at PS.Security@sbp.org.pk .

4.2. Security Control Implementation & Monitoring

The process of Security Control Implementation and Monitoring includes formal arrangements made to implement security control and monitoring mechanism to prevent, detect and correct security gaps identified during security risk assessment. CSPs shall also ensure accountability by designing policies, controls and SOPs including but not limited to the following:

a. CSPs shall implement EMV standard on all Payment Cards and the related infrastructure that process Payment Card transactions by June 30, 2018. In this regard, CSPs shall not pass on EMV re-carding charges to their consumers.
b. CSPs shall implement authentication measures like Two/ Three Factor authentication etc for Payment Card transactions to authenticate the identity of cardholders and to cater the non-repudiation risk.
c. CSPs shall preferably comply with PCI DSS and PA DSS standards.
d. CSPs shall implement automated solutions to monitor and proactively track fraudulent usage of Payment Cards.
e. CSPs shall implement transaction limits and other related security controls for stakeholders i.e. consumers, merchants etc that commensurate with their risk profile.
f. CSPs shall ensure that photo identity is checked for all non-EMV Payment Cards at merchant locations for POS transactions.
g. CSPs shall ensure that receipts are invariably generated for transactions conducted through Payment Cards. Further, consumer shall immediately receive a mobile SMS on registered cell number or an email may be sent on registered email address whenever a transaction is made using Payment Card.
h. CSPs shall ensure traceability of transactions through appropriate audit logs.
i. CSPs shall ensure confidentiality of consumers' data in storage, transmission and processing as per relevant applicable legal framework.
j. CSPs shall install appropriate security mechanisms like Anti-skimming and Biometric devices etc on their ATMs and POS machines.
k. CSPs shall train merchants about security measures required for executing Payment Card based transactions on POS and other related infrastructure e.g. cross checking of CNIC before executing transactions etc.

l. CSPs shall perform proper due diligence of the merchants before taking them onboard and maintain a complete record of details i.e. registration, location, address, contact details etc.

m. CSPs shall have their Payment Card based systems audited annually through external auditor.

n. CSPs shall ensure risk mitigation through well defined SLAs for systems that are outsourced to vendors.

o. CSPs shall formally define and document security and contractual responsibilities of all stakeholders i.e. consumers, payment schemes, third party vendors etc who have access to their systems and data and communicate the same to relevant stakeholders accordingly.

4.2.1. Fraud Resolution Management

a. CSPs shall put in place a FRM mechanism that shall assess, monitor and regularly review types of frauds and complaints relating to Payment Cards.

b. CSPs shall ensure that FRM shall include measures to address fraud issues and take prompt actions to resolve the same.

c. CSPs shall coordinate with other stakeholders on the identification of a fraud and take prompt action to prevent it from further spread.

d. FRM shall recommend Payment Card security measures on the basis of nature of the complaints/ issues reported and shall incorporate the same in their TORs and SOPs.

4.2.2. Dispute Resolution Management

a. CSPs shall establish Dispute Resolution Center (DRC) and deploy adequate human resources to address consumer complaints with a well defined TAT for their resolution.

b. CSPs shall ensure that the Call Center/ Helpdesk/ IVR services are available to the consumers 24/7 to report complaint, fraud, identity theft etc.

c. CSPs shall establish and manage complaint reporting, tracking and resolution system.

4.2.3. Card Issuance

a. CSPs shall not issue unsolicited Payment Cards to their accountholders and shall take consumer's consent for Payment Card issuance in writing or through other electronic channels using their registered numbers, emails and digitally captured signatures etc.

b. CSPs shall take consumer consent regarding the utilization of Payment Cards on various ADCs or their cross border usage while maintaining the record of consent as per SBP record retention policy.

c. CSPs shall ensure that the Payment Cards issued to the consumers are personalized i.e. the cardholder name shall be embossed in English language at the time of issuance.

4.2.4. Card Delivery & Activation

a. CSPs shall maintain strong controls for management of inventory for the issued and non-issued Payment Cards.

b. CSPs shall ensure that secure procedures are adopted for activation of new and replaced Payment Cards.

c. CSPs shall dispatch inactive Payment Cards to their consumers at their registered addresses through registered courier services. In case of delivery of Payment Card to consumer at branch, the CSP shall perform due verification of consumer.

d. CSPs shall activate Payment Card at the branch upon in-person request by the cardholder or on receipt of call from cardholder's registered contact number.

e. Call Center and IVR shall be capable of interacting in English and Urdu languages. Regional languages shall also be considered for communication with consumers.

5. Consumer Awareness & Record Retention

a. CSPs shall develop and implement a formal consumer awareness program regarding safe usage of Payment Card and NPMs, while highlighting risks and frauds associated with them.

b. CSPs shall clearly communicate the explanation of liabilities, roles and responsibilities of consumers for using Payment Cards in Urdu and English languages. Regional languages shall also be considered for communication with consumers.

c. CSPs shall keep the complete record of Payment Card activation, PIN generation, consumer's written/ digital consent for Payment Card issuance and usage on ADCs and complete transaction details for a period not less than ten years in secure and confidential manner.

d. CSPs shall maintain complete visual records of all ATM transactions for a period of one year.

e. CSP shall take necessary contingency measures in terms of alternate telephone numbers if Call Center/ Helpdesk/ IVR become temporarily non-operational.

f. CSPs shall provide transactional data to consumers as and when requested.

g. CSPs shall inform SBP as well as consumers at least two weeks earlier if any maintenance, up-gradation, switch-over activity and/ or any change management activity is conducted and the same may result in downtime of Payment Card based systems.

6. Roadmap for EMV Compliance

a. ATMs, POS and other related Payment Card processing infrastructure shall be compliant with EMV standard by December 31, 2017.

b. CSPs shall begin to issue Europay MasterCard Visa (EMV) Payment Cards from June 30, 2018 onwards.
c. All Payment Card processing infrastructure shall accept Chip and PIN by December 31, 2018.

Annexure A: Report on Data Breaches

Card Data Security Breach Report							
Name of CSP: _____							
Date: DD-MM-YYYY							
S. No	**Number of Cards Compromised**	**Merchant or Bank system where Card Breach Occurred**	**Volume of Compromised Cards**	**Value of Compromised Cards**	**Nature of Breach**	**Action taken to rectify security breach**	**Remarks**

Submitted By (Official's Name):_____

Designation: _____

Contact Number: _____

Document Ends

****