Techniques and Security Measures for Fraud Prevention in Payment cards

Pankaj Richhariya¹1, Dr Prashant Kumar Singh²

¹Computer Science Department, Dr K.N.M.U University
Rajasthan, (Newai) India

Abstract—Effective fraud prevention can transform business performance for financial services organizations. Implementing a comprehensive and structured program to prevent fraud has become a core driver in business growth, delivering real competitive advantage. In this paper we manage fraud related to multiple products from a single platform, and take a card, account and customer-level and transaction level view of fraud cases and discusses the various fraud prevention techniques and other security measures that are necessary.

Keywords— Fraud prevention, Transactions, Payment System, Security.

1. Introduction

With the widespread use of increasingly advanced Internet technology [4, 5, 6], online banking (also called Internet banking) is emerging as a major channel for retail and business banking. As fraud increases dramatically with the expansion of modern technologies, there is an urgent need that sophisticated technologies and fraud experts’ knowledge should be combined in order to ensure against fraud attacks. In past, banks members of payment system had solved fraud prevention problems by means of organizational measures: limits on numbers and amounts of cardholder’s operations, monitoring of transactions in high risk countries, use of various methods for card verifications, etc. [2][3]. There are limited papers about fraud control in online banking [7, 8, 9]. The mainstream online banking fraud detection systems rely on domain experts and knowledge to create rules for filtering suspicious transactions, which face critical problems nowadays, individuals, organizations or companies apply various fraud prevention methods, aiming at minimizing their losses as soon as possible.

In particular, fraud prevention involves measures to inhibit fraud at an early stage, such as personal identification number for bank cards, chip-based EMV payment cards, Internet security systems for credit card transactions, Subscriber Identity Module (SIM) cards for mobile phones, laminated metal strips and holographs on banknotes etc. However, none of these measures acts as a panacea in practice. What is more, there should be a trade-off between expense and inconvenience (e.g. to a customer) on the one hand and effectiveness on the other. According to the theory and practice of risk management, each bank has to implement special measures in order to prevent fraud in time [1]. There is the necessity of an effective system that prevents and detects frauds effectively with zero loss exists awaiting now. Both users and fraudster are influenced due to the development of new technologies day to day. Therefore, in this scenario, it becomes compulsory that the users required keeping on a step ahead. The various techniques of fraud prevention from the profile (account) creation to the transaction processing (auth system) and the various security measures for the fraud prevention.

2 Fraud Prevention Techniques

To reduce the fraud risk and misconduct from occurring it is necessary to prevent the fraud from account creation to the transaction processing. There are some fraud prevention techniques given below:

2.1 Fraud prevention in profile (account) creation

During the profile (account) creation of any customer in the bank, the number of measures given below bank has to take place to prevent the fraud.

(i) Authentic Document submission

To establish identity, the bank always requires an authentic document that carries photo of the customer such as passport /driving license/ pan card/ voters’ card etc. The residential address of the customer that these documents contain may not be the customer’s present address. Therefore, Telephone/Electricity bill etc. is added with the driving license /passport/ pan card / voters’ card in order to record the current address of the customer.

Following are the described list of the documents that the bank can ask for identification:

Table 1.1 List of documents banks required for identification

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passport</td>
<td></td>
</tr>
<tr>
<td>Driving License</td>
<td></td>
</tr>
<tr>
<td>Voter Card</td>
<td></td>
</tr>
<tr>
<td>PAN Card</td>
<td></td>
</tr>
<tr>
<td>Address Proof</td>
<td>(any document which provides customer identification of the satisfaction of bank)</td>
</tr>
<tr>
<td>SIM Card</td>
<td>(any number which provides customer identification of the satisfaction of bank)</td>
</tr>
<tr>
<td>Bank account</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from any recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
<tr>
<td>Letter from a recognized public authority</td>
<td></td>
</tr>
</tbody>
</table>

(ii) Proper identification procedure

Customer identification is used to identify the customer and verify his/her identity by using reliable...
multiple source documents, information or data. Banks have been advised to check the Customer Identification at different stages for example at the time of establishing a banking relationship; carrying out a various financial transaction or whenever the bank has a doubt about the consistency/ authenticity or the inconsisteny of the previously obtained customer identification data. Identification should be automated and verified regularly on all customer profile.

(iii) Full KYC procedure to be followed

KYC is an abbreviated as “Know your Customer”, used by the banks for customer identification. KYC has two components - Customer Identity and Customer’s Address. The banks are required to update customer records infrequent time intervals because in many cases the customer’s address may change having the same identity.

Identification process involves efforts to determine real identity and ownership of accounts, the type of customer’s business, the source of earning funds, relation between the customer’s business and the operation of account, etc. This all help the banks to manage their risks. The objective of the Know your customer (KYC) guidelines is to prevent banks by criminal elements that are being used, intentionally or unintentionally for money laundering. The Application of full KYC procedure is compulsory before issuing Smart Cards/ Debit Cards /Credit Cards/ add-on/ supplementary cards.

(iv) Regularly Monitoring Customer detail

Based on the risk type of the customers banks always have been advised to update the customer identification data in frequent time slots in order to make sure that the current details about the customer are available.

Banks maintain a customer profile based on data provided by the customer like financial or Social status, nature and information about customer’s business with their location, sources of wealth or income, the purpose of opening the account, the expected sources of the funds that is being used in the relationship and occupation details, expected monthly withdrawals, expected monthly remittance, etc. If the transactions in the account are observed inconsistent with the profile provided by the customer, the bank has right to ask for any other additional details / documents as per their requirement. The purpose of this is to confirm that the account is not being used for any Criminal activities /Money Laundering/Terrorist.

(v) Correct Email Address & Mobile number

The transaction done by the customer (the amount is debited/credited), or authentication required for OTP, or the password changed etc. whatever communication is done by the bank to the customer is through the Email address and mobile number. So that the correct email address and mobile number to be filled during the creation of an account by which the secure communication can be done and can be prevented from fraud.

2.2 Fraud prevention in transaction processing (auth system)

If it is manually reviewed that whether online or offline payment transactions are fraudulent or genuine, it takes a lot of time and effort. So, to evaluate that whether a credit card transaction is authenticated or fraudulent, it is necessary that the process needs to be updated with the aid of a fraud monitoring and its prevention system that is capable of analyzing different parameters and process it. In order to detect and prevent online or offline fraud, Payment Alert processes have used that checks each transaction payment transaction with widespread risk parameters. Different parameters are analyzed in order to evaluate a wide range of fraud patterns. There is different risk parameters payment alert use to evaluate the risk of transactions online or offline in real-time is given below.

(i) Card Validation Check

In the card validation check, it is ensuring that the name and the card number is checked. Whether the name on the card and the account holder name are the same. If not, the merchant can cancel the transaction and deny additional purchases.

Credit card validation checks detect errors in a sequence of numbers, so it easily detects valid an invalid numbers. The credit card number is validated using the luhn algorithm, if the result of validation is true then the number will be considered as valid, and another check will be executed, else the transaction won’t be allowed.

(ii) PIN Check for Secure Authentication

This check is for the authentication process, payer authentication is a new technology introduce a new level of security to B2C (business-to-consumer) internet commerce. This type of service first implemented as VbV (Verified by Visa) or VPAS (Visa Payer Authentication Service) program that was launched worldwide in 2002 by Visa. Similar to use with ATM cards this program likewise depends on a Personal Identification Number (PIN) allied with the card and establish a secure direct authentication channel between the issuing bank and the customer. The PIN is issued associated with the specific card by the bank at that time when the cardholder enrolls the card with the program and will be used to authorize online transactions.

When registered cardholders appear at a participating vender’s place, they will be led by their issuing bank to provide their PIN relevant with that card. When the password is verified, the merchant can be able to complete the required transaction and then transmit the information of verification on to their acquirer. Now a day various authentication are used for security some of them discussed later:

(iii) Card Status Check

The Card Status Check keeps in the priority of the rules which is discussed later. In this check, the status of the card is checked whether the card is active or inactive or blocked it also checked that whether it
has been reported as a lost credit card or stolen credit card by the cardholder. If the above check is true then transaction won’t be allowed, else another check will be executed. This type of check makes it easier to stop fraudulent transactions.

(iv) AVS check
Address verification system is used in the online transaction or card-not-present situations. Address Verification System (AVS) match the first few characters/ digits of the street address and the PIN code information was given by the customers for delivering/billing the purchase to the relevant information on record with the card issuers. The Code that does not represent the level of match between these addresses is returned back to the merchant. In the case of international transactions, AVS is not much useful.

(v) CVV check
The Card Verification Method3 (CVM) contain 3/4-digit numeric code that is printed on the card but neither is punched on the card nor is available in the magnetic stripe of the card. The merchant can appeal the cardholder to provide this 3 or 4 digits numeric code in case of the card less transaction and submit it with authorization. The objective of CVM is to make sure that the person doing the transaction is an authorized one. Also, the code cannot be skimmed from the magnetic stripe or copied from receipts. CVM also provides some protection for the merchant, but it never helps them from the transactions that are placed on physically stolen cards. Moreover, fraudsters who have temporary control of a card can be able to read and copy the CVM code.

(vi) Parameter Format Checking
This system will assess the customer information and evaluate the genuineness of the order based on the details provided by the customer such as information of credit card, contact number and email address and checks the database for discrepancies. Credit card numbers are used to determine if the credit card is valid or not until present. Paid or office email address has a lesser chance of being fraudulent than a free email address. Contact numbers are cross-checked to determine if it is in the similar country as the address of billing that is provided or not.

(vii) Blacklist Control
Both MasterCard and Visa gives a list of merchants who have been being there comprised of the transactions that are fraudulent earlier. Now these lists can provide useful information to acquirer’s right at the time of vendor employment preventing probable fraudulent transactions.

Payment Alert maintains a blacklist database of credit cards checks whether the transaction came from a card number, card bin, IP address, or email that are present in the blacklist database are discarded by the system when they used in a payment transaction. The card that was previously reported as stolen, used for unauthorized transactions, or originate from a high-risk country are put in the blacklist database. The customers are allowed to add their own entries they wish to do so. The information that is analyzed is: IP address, Email-ID, Card Number etc.

(viii) Geographical Checking
It identifies the source of the transaction by its IP address and checks if it’s reliable with the provided information such as country, settings of languages, and time region and matched with the data that is ordered such as billing and shipping address in turn to review the transaction using:

- High-Risk Country Control – When transaction came from the high-risk country than System will consider a transaction risky or dangerous.
- Country Mismatch Checking – If there is any difference between billing and delivery address than the system will consider a transaction risky.
- Language and IP Checking – If language settings of the computer are distinct with the position of the IP address that system will consider a transaction as risky.
- Time Zone and IP Checking - If in the computer the time settings are different with the position of the IP address system will consider a transaction as risky.

(ix) Velocity Checking
The system can calculate and assess doubtful transactions exhibiting unusual buying behavior and these checks are used to defend vendors and decrease fraud by allowing them to fix transaction frequency limits and card handling within a definite time slot. These features allow merchants to be alert when there are probable cases of fraud because of unusual buying behaviors such as:

- In the span of 30 minutes, the same card is used for buying 10 times.
- Multiple orders are placed using different cards but all are shipped to the same address
- From the same IP address multiple orders placed using different cards, names, and addresses.
- Frequency of orders from the same URL.

(x) Transaction Limit Checking
Similar to Velocity Checking, Transaction Limit checking emphases more on the frequency of transactions and amount. The transaction limit checking helps to prevent the possible circumstances of a fraudster ask for many items of a costly item sets a daily/weekly/monthly processing limit in order to prevent abnormal buying behavior.

(xi) Historical Negative Record Checking
The system can check the historical transaction data that contain negative records in order to block any card or IP address. For further future reference, the outcomes of every transaction made by payment card are stored in a database whenever an online payment transaction is made. The cards that are discovered as fraudulent are stored in the database because if again in future that card was used for the transaction, it will be flagged for further review. Beside from the outcomes of the transaction, cards with surplus
chargebacks are also considered as high-risk transactions because they may have been the cases of friendly fraud.

(xii) Risk Scoring

Every risk parameters can be allotted a customized weight level in order to give more importance to risk parameters to oppose certain fraud patterns that are more common in businesses. Businesses have numerous requirements and operate under various situations and each has exclusive experience with online fraud. To assist businesses, one of Payment Alert’s key features is its Risk scoring that allowing vendors to set their threshold for risk levels.

In addition, according to risk parameters that have more impact on their industries merchants can give that parameter heavier weight. This helps merchants to detect fraud by optimizing the performance of electronic Payment Alert.

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>..</td>
</tr>
<tr>
<td>High</td>
<td>1400 to 1999</td>
</tr>
<tr>
<td>Medium</td>
<td>600 to 1399</td>
</tr>
<tr>
<td>Low</td>
<td>1 to 599</td>
</tr>
</tbody>
</table>

Figure 1.1 Setting for rules for risk level

(xiii) Customizable Rules

To get the best protect from the fraudulent transactions, the alert system can also develop the specific rules that can be customizable i.e. the various rule can be customized by vendors might need.

(xiv) Lockout mechanisms

Automatic card number generators represent one of the new scientific tool generally used by fraudsters because these programs can easily retrieve from the internet, are able to generate thousands of credit card numbers that are valid. The frauds behavior originated through a card number generator are following:

- Multiple transactions having similar card numbers for e.g. same Bank Identification Number (BIN)
- A large number of declines

2.3 Other Security Measures for Fraud Prevention

(i) Secure the Network

By Use of Firewalls

All systems must be protected from access that is not authorized from the networks that is totally untrusted, whether at the time of using the internet for e-commerce, Internet access through the browsers present in desktop of employee, e-mail accessing of employee, using dedicated connections such as B2Bi (business-to-business) connections, by wireless networks or by other sources. Often, seemingly irrelevant paths to and from the networks that are not trusted can provide unprotected pathways into systems. When Firewalls is used the in system it provides a protection mechanism for any computer network.

Firewalls are devices that monitor computer traffic passing between an internal networks and external networks those are not trusted, as well as traffic goes out and in of more sensitive areas within an entity’s internal networks that are trusted. Within an entity’s trusted network example of a more sensitive area is the cardholder data environment. Firewalls stop any suspicious data before it enters in our system;

Firewall offers great advantages in the field of security but still has its limits: the main reason is that its port can never be closed. At least, it must have even one open port to communicate with the Internet and this single port can be considered as a door for attacks. This means that any time our computer may be under attack [65]. A firewall has the special property that it checks all network traffic that passes through it and restricts those transactions that do not meet the particular security criteria mentioned in its database.

Do not use Default password for system

To compromise the security of system malicious individuals (external and internal to a company) regularly use vendor default passwords and other vendor default settings. By hacker communities, these passwords and settings are well known and easily determined via public information. During installation databases lock and expire default accounts and passwords. At that time, Passwords for administration accounts are prompted. And the database Access Manager includes self-service password reset with policies that can meet the requirements.

(ii) Monitoring and testing networks regularly

Logging procedures and the capability to track user behaviors are critical in preventing, detecting, or reducing the influence of a data compromise. The existence of logs in entire surroundings allows detailed tracking, warning, and analysis when anything going illegal.

- Implement audit trails to link all access to system components to each individual user. And employing automated audit trails for all system modules to rebuild the events given below:
  - Separate user accesses to cardholder data and all deeds taken by any person with administrative privileges
  - Access to all review trails Illegal logical access attempts and Use of and changes to identification and authentication mechanisms including but not limited to the creation of new accounts and elevation of privileges and all modifications, additions, or deletions to accounts with root or administrative privileges. And in system-level entities Creation and deletion.

- However, For every event recording the following audit trail entries for all system components:
  - Identification of the user, Type and origination of the event, Time and Date
• Indication for the Success or failure, Identity of influenced data, system module, or resource

➢ All the audit trails must be secure so that they cannot be changed.

• Limit seeing of audit trails to those with a task associated requirement. And preventing files of audit trail illegal alterations.

• Instantly back-up audit trail files to a centralized log server that is tough to change. And to confirm that current log data cannot be altered without producing warnings (while new data be there added should not produce the warning) use file-integrity checking or alter-detection software on logs.

➢ Review logs and security events for all system components to identify anomalies or suspicious activity and keeping the history of an audit trail for as a minimum one year, and for analysis instantly obtainable with a minimum of three months.

(iii) Maintaining Policies of Information Security

To address the information security for all personnel, it is one of the most important requirement to maintain policies. A strong security strategy puts the security quality of the entire entity and notifies staffs what is likely of them. Entire staffs should be conscious of the sensitivity of data and their accountabilities for preventing it. Determine, look after and expand security strategies that achieve the following:

➢ Focuses on all PCI DSS necessities. And including to process annually that recognizes threats, and susceptibilities, and consequences in a formal risk assessment. Also comprises a review when the situations altered at least annually and updates.

➢ Acquire day-to-day functioning security measures that are compatible with necessities in this specification (for e.g., maintenance of user account measures, and log analysis measures).

➢ For critical technologies defining and developing the proper usage strategies of technologies (for e.g., wireless, remote access, removable media, tablets, smartphones, personal digital assistants, e-mail usage and Internet usage). Confirming these usage strategies need the following:

- For the use of technology authentication and clear approval by authorized persons, technologies use and Acceptable network location technologies.

- For remote access when there is not any activity automatic disconnection of sessions. i.e. instantly deactivation after use.

- For personnel accessing data of cardholder by remote-access, prohibit the storage of data on local hard and removable media, until clear authorized for a defined industry need.

➢ Accountability of all the personnel must be ensured clearly security strategies and procedures for security information. And also assigning role and responsibility to an individual or team. The following are the accountabilities of information security management:

• Creating the document and distribute security strategies and procedures.

• Analyze and monitor security information, warnings and deliver to suitable personnel.

• Monitor and control all access to data. The account of Administrator user comprising modifications, additions and deletions

➢ Prepare all staff to aware of the significance of cardholder data security Implement a program for security awareness. And execute an event response strategy. Be ready to respond instantly to a system contravention. Confirm that strategy addresses the following, at least:

• Notification of the payment makes at least included in the event of compromise of Roles, responsibilities, and communication and contact strategies and Particular instance response, business recovery and continuity procedures

• Analysis of legal requirements for reporting compromises. And Data back-up processes, Covering and responses all the modules of critical system with the Situation or inclusion of event response measures from the payment makes

• Appoint particular personnel respond to alerts and available on a 24/7 and at least annually test the plan at least annually and delivering the suitable training to staff with security breach response responsibilities.

(iv) Preserving Cardholder Data

Prevention methods such as hashing, encryption, masking, and truncation are critical modules of cardholder data prevention. If an impostor evades other controls of security and gets access to the data which encrypted, without the appropriate cryptographic keys, the data is not readable and useless to that person. To protect stored data other efficient methods should also be thought of probable risk mitigation chances. For e.g., methods for reducing risk comprise data of card holder are not stored unless completely necessary, if complete PAN is not require truncating the data of cardholder, and not send out insecure PANs by end-user messaging technologies, such as email-id and instant messaging.

• When PAN displayed it must be masked (the number to displayed are first six and last four digits are the maximum), such that only personnel with a genuine business require to see the complete PAN.

• Provide PAN unreadable anyplace it is stored.
• Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:
  Limited access to cryptographic keys to the least number of protectors essential. Nobody needs access to the master encryption key. Designated individuals like a DBA or Database Security Administrator (DSA) need to know the wallet password or the HSM authentication string and have the ‘alter system’ privilege in order to open the wallet or HSM and make the master encryption key available to the database. Command rules can be implemented to restrict who, when, and where the ‘alter system’ command can be executed.

(v) Managing Vulnerability Program
Malicious software commonly referred to as —malware—including viruses, worms, and Trojans—enters the network through many businesses accepted activities comprising email of employee and internet use, smartphones, laptops, and storage devices, resulting in the misuse of system susceptibilities. To protect systems from existing and growing malicious software risks anti-virus software should be used on all systems usually affected by malware.

• Use anti-virus software on all systems usually affected by malicious software (mainly servers and personal computers). And ensure that all anti-virus are proficient of detecting, removing, and defending against all malicious software
• Confirming that mechanism of anti-virus are recent, updated, running actively, and creating audit logs.

To preserve protected systems and applications dishonest persons use security susceptibilities to acquire privileged access to systems. A lot of these susceptibilities are fixed by the merchant -provided security patches, which should be installed by the persons that govern the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by

➢ Establishing a procedure to recognize security vulnerabilities, using reliable external sources for security vulnerability data, and allot a risk ranking (for e.g., as “high,” medium,” or “low”) to newly discovered security vulnerabilities.
➢ Confirm that all system modules and software are safeguarded from recognized susceptibilities by installing all merchant provided security patches. Within one month of release, install all critical security patches.
➢ All the alteration made by the system module follow alteration control processes and measures. The processes must comprise the following:

• Segregate development/test domain from creation domain, and apply the segregate with access controls and segregation of duties among development/test and creation domain.
• Created data (live PANs) are not used for testing or development
• Alteration control measures for the implementation of software alterations and security patches alterations should comprise the documented change approval by authorized parties
➢ Address standard coding susceptibilities in the processes software development as follows:

• Insecure coding techniques train the developer, comprising how to prevent standard coding susceptibilities, and understanding by what means sensitive data is carried out in memory.
• Develop applications based on secure coding guidelines.

(vi) Execute Strong Access Control Measures
It must be ensured that the data which is very critical can only be accessed by authorized staff, corresponding to the job responsibilities the systems and processes must be in place to limit access based on the requirement to know. When access rights are granted to only the minimum amount of data and privileges required performing a job.

➢ The cardholder data and components of the system must be limited access to those persons only whose roles requires such access. And Limit access to privileged user IDs to minimum privileges essential to accomplish job accountabilities. Define access needs for each role, including:

• System components and data resources that each role needs to access for their job function
• The level of privilege required (for example, user, administrator, etc.) for accessing resources.

➢ Create an access control system for systems modules with various users that limit access based on a user's required to know, and until the specifically permitted it is set to “deny all”. The following are the access control system that must include are:

• Coverage of all system components. And according to job classification and function, the privileges are assigned
• The setting is default “deny-all”
  Only through the programmatic methods all user access to user queries of, and user actions on databases are through programmatic methods. And only database administrators have the ability to directly access or query databases.

3. CONCLUSION
In this chapter, we represent the financial fraud prevention techniques and various security measures. From the profile (account) creation to the complete transaction process which necessary preventive
measures the financial organization have to be followed to prevent the fraud. And Fraud prevention in transaction processing (authorization system) which security checks and the other security measures are mandatory to prevent the fraud.

ACKNOWLEDGEMENT
The authors wish to thank Mr. Satendra Jain, SATI Engineering College Vidisha for providing the guideline in this Contest.

References: