Card Acceptance Guide

Released September 2024

Version 1

To visit the IL State Treasurer's Office ePAY site please click here

Table of Contents

Section 1: Who takes part in the Credit Card Payment Process?

1a: ***Who are the Card Brands and why are they important?***

Section 2: The Credit Card Transaction Process

2a: How does a Merchant get funded?

2b: ***Retention of Sales Drafts***

2c: ***Charging a Service Fee***

2d: ***How long does a credit card payment take to process?***

2e: ***Processing a refund***

2f: ***What Happens When a Credit Card Transaction Gets Declined?***

2g: ***Prohibited Transactions***

Section 3: Credit Card Transactions and PCI Compliance

3a: ***What is PCI-DSS?***

3b: ***The PCI Data Security Standard***

3c: ***The 12 Requirements of PCI DSS***

3d: ***What is Cardholder Data?***

3e: ***What Cardholder Data Can and Cannot Be Stored?***

3f: ***PCI Data Storage Do's and Don'ts***

Section 4: What is a Credit Card Chargeback?

4a: ***Reasons for Chargebacks***

4b: ***Dos and Don'ts***

4c: ***Why are Credit Card Chargebacks bad for business?***

4d: ***How can businesses reduce Chargeback Fraud?***

Section 5: Fraud Prevention

5a: ***Common types of Fraud***

5b: ***Best practices of how to prevent Fraud***

Section 6: How do Online Payment methods stay secure?

6a: ***Completing Electronic Commerce Transactions***

6b: ***How Do eCommerce Transactions stay secure?***

---

i: Introduction

The Payments Card Acceptance Guide was created to provide ePAY Participants with a reference tool for important payment processing and industry information. The content included should be used as a guide for accepting payments.

ii: The Purpose of this guide

Today's Government Participants are accepting and demanding more complex ways to accept electronic payments. Whether it be a standard POS Stand-Alone Credit Card Terminals or a complex Third-Party Integration, accepting transactions in the various ways that allow government clients to operate is crucial to day-to-day operations.

Global Payments' Card Acceptance Guide is a guide for all Illinois ePAY Participants that accept card-present and online transactions.

The purpose of this guide is to:

1. Provide Participants and their staff with an overview of accepting card-present and online transactions.

2. Provide guidance and best practices for accepting payments.

3. Provide guidelines and best practices for avoiding fraud when accepting payments.

iii: Global Payments – A Payment Processing Partner

Welcome, and thank you for choosing the ePAY Program for your payment processing. The chart below indicates how many Agencies, Universities, Cities, Villages, and more use and trust the ePAY Program to manage the important task of handling their POS and web payments.

Global Payments, in partnership with the ePAY team, process billions of credit, debit and electronic check transactions. These Participants trust the ePAY team to manage their processing and POS needs and have done so for over 22 years.

As of January 2024 ePAY Participants Include:

38 State Agencies	18 Universities/Colleges
31 County Agencies	68 Libraries & Library Districts
194 Cities & Villages	6 Parks & Rec Facilities
18 Water/Sewer Districts	7 Public Transportation
7 Soil & Water Conservation Districts	22 Public Health & Safety
92 Schools and Board of Education Offices	3 Townships

iv: Global Payments' role

Global Payments' most important role is serving as a valued partner with the Illinois State Treasurer's Office ePAY Team providing quality products and services to the Participants of the Illinois State Treasurer's ePAY Program. Global Payments is committed to providing an elevated level of service, value, and a comprehensive selection of POS and eCommerce solutions for fast, dependable, and secure processing and settlement.

Global Payments offers many years of experience in payment processing and is a full-service provider of Merchant Processing Services for:

All major Credit Cards

Signature Debit Cards

Pin Debit Cards

*EBT cards**

Commercial Cards

Gift Cards

Purchasing Cards

*Available and typically not used for government payments

Global Payments offers a full range of Merchant Processing Services in both traditional transaction processing and emerging payment technologies, including:

Card authorization

Draft capture

Chargeback handling

eCheck verification

Credit card processing

Debit card processing

Electronic benefits transfer processing (EBT)

Help desk

Merchant accounting

Reconciliation

Settlement

Terminal management & support

Web-based transactions

Web-based reporting services

v: Participant's role

As a Global Payments/ePAY Program Participant, it is important to:

1. Read, understand, and abide by the *Participant Merchant Agreement* and this Card Acceptance Guide.

2. Take all necessary steps to prevent fraud.

3. Follow best practices in accepting electronic payments.

4. Advise the ePAY Team of any changes related to the participant's business, such as changes in status, changes in business structure, address or contact information, or cancellations.

5. Notify the ePAY Team upon canceling or returning equipment.

6. Keep up to date on all industry news and policy changes.

7. Advise the ePAY Team of any changes to Merchant Payment Application, hardware, or software.

NOTE: *It is a Participant's responsibility to comply with all applicable laws and association rules and regulations. Please note that, while several guidelines in this Card Acceptance Guide reference or suggest obtaining certain information from a Cardholder in the transaction process, Participants should consider and are responsible for compliance with any applicable state laws regarding obtaining personal information from a Cardholder in connection with a card transaction.*

Need Assistance?

Global Payments and the Illinois ePAY Team are here to help. The ePAY Home Page is also a source of information regarding the ePAY Program's products and services. To access the website, go to:

ePAY Home Page – https://illinoistreasurer.gov/Local_Governments/ePAY_Overview.

For information about additional products and services available through the ePAY Program, please **call: 855.226.7337** or **email:** ePAYCustomerSupport@illinoistreasurer.gov

---

Section 1: Who takes part in the credit card payment process?

It sounds easy – a Consumer hands a Credit Card to a Merchant and buys a product or service. The money is debited from the Customer's account and credited to the Merchant's account.

It happens millions of times each day. But how? Who plays what role in the business process that happens behind the curtain?

In this section and accompanying infographic, you will see the role that ePAY's contracted processor plays in the credit card transaction lifecycle. This includes the Payment Application Provider, the (Front-End) Processor, and Transaction Gateway. Our parent company, Global Payments, Inc., serves as the Back-End Processor and works directly with the Card Brands.

And remember – this all happens in a matter of a few seconds.

The players involved in the payment process include:

Constituent (Cardholder): The "Constituent" is a person or entity that utilizes the ePAY Program to make payments or donations of public funds to a Participant. In many cases, for the purpose of discussing a credit card transaction, we may use the term "Cardholder" which is the customer that presents their card for payment of goods or services. These two terms often may be synonymous when discussing the ePAY Program and payment acceptance.

Participant (Merchant): The "Participant" is the State Agency, Municipality or Government Entity that sells goods or services. In many cases, for the purpose of discussing a credit card transaction, we may use the term "Merchant" which is the entity that presents goods or services for sale to Cardholders. These two terms often may be synonymous when discussing the ePAY Program and payment acceptance.

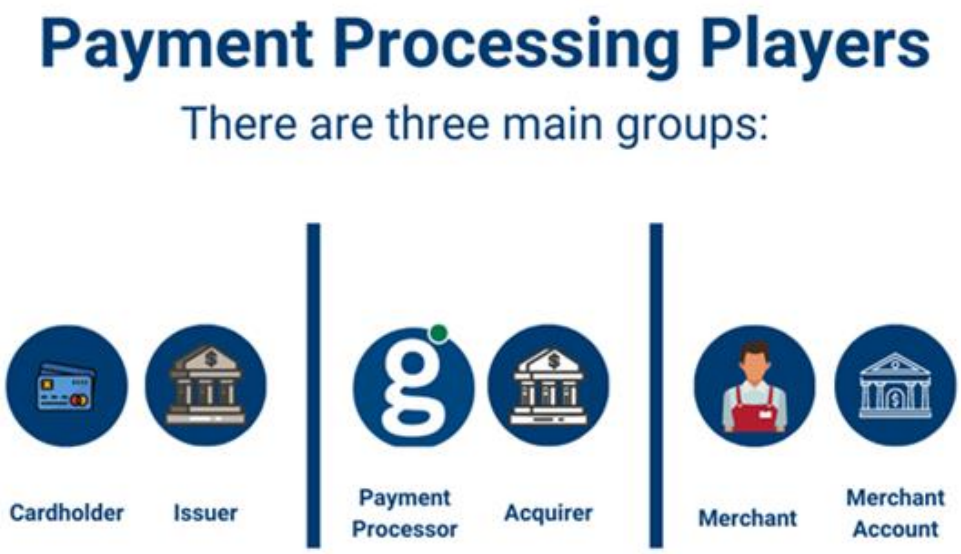
Issuer: The Issuer (or "Issuing Bank") provides the Cardholder with their credit and a physical card. They are responsible for approving and declining transactions, customer billing, and collections.

Merchant Account: This is a type of bank account that allows businesses to accept credit cards, debit cards, and Mobile Payments.

Acquirer: An Acquirer (or "Acquiring Bank") solicits, underwrites, and owns the accounts Participant (Merchants) need to accept credit cards. They can provide the technology permitting businesses to process transactions, take on chargeback risk, and deposit funds into a Merchant's bank account.

Payment Processor: Payment Processors are organizations that partner with Acquirers to open Merchant accounts, handle support, manage payment processing, and build technology on behalf of Acquirers.

Card Brands: A Card Brand (sometimes called a Card Network or Association) is an organization that facilitates payment card transactions. See further information below regarding the importance of the Card Brand.



1a: Who are the Card Brands and why are they important?

As stated, the Card Brand is sometimes called a "Card Network" or "Association." The Card Brands do indeed facilitate payment card transactions. They also regulate who, where, and how cards are used. Examples of Card Brands include Visa®, Mastercard®, American Express®, Discover®, China UnionPay®, and JCB®. Card Brands also partner with Card Issuing Banks to market their branded credit cards to the public. As part of the marketing efforts, Card Issuing Banks and the Card Brands will offer incentives like "Cash Back" or "Loyalty Points" to attract or retain new and existing card holders.

To summarize, Card Brands partner with the Issuer to offer physical credit cards to Constituents. For more information on the Card Brands and how they operate in the payment eco-system, please visit the links below:

https://usa.visa.com/

https://www.mastercard.us/en-us.html

https://www.discover.com/

https://www.americanexpress.com/

Note: Some Card Brands have partnerships with Mastercard and Discover and operate on the Mastercard and Discover platforms yet have their own branding. China UnionPay®, and JCB® are examples of these co-hosted Card Brands.

Section 2: The Credit Card Transaction Process

These 10 steps show the credit card transaction process:

1. The Cardholder initiates a purchase

The Credit Card Transaction Process begins when the Cardholder presents their credit card for payment. They may enter the card information online, swipe or insert their credit card, or simply tap if they have EMV contactless capabilities.

2. The Merchant requests authorization after processing the card information

From here, the Merchant's bank processes the card information and then requests authorization from the appropriate credit card network, such as American Express, Discover, MasterCard, or Visa.

3. The Payment Gateway routes card information to the Processor

The Credit Card Issuer authorizes the transaction by sending back a unique code. If the credit card is declined, the customer will get a message at the point of sale or during the online transaction process.

4. The Processor, Global Payments, submits an authorization request to the Credit Card Association

Next, Global Payments submits an authorization request, which includes the credit card details and transaction details to the Credit Card Association.

5. The Card Brand submits an authorization request to the Issuing Bank

An authorization request is sent from the Card Brand to the Issuing Bank and includes the credit card number, card expiration date, billing address, card security code, and the payment amount.

6. The Issuing Bank approves the authorization request

Once received, the Issuing Bank reviews the request and either approves or denies the transaction. A response is sent to the Merchant via the same channels.

7. The Card Brand routes the authorization to the Acquiring Bank

If the transaction is approved, the Participant receives an authorization, and the Issuing Bank places a hold for the amount of the purchase on the Constituent's account.

8. The Acquiring Bank forwards the authorization to the Merchant

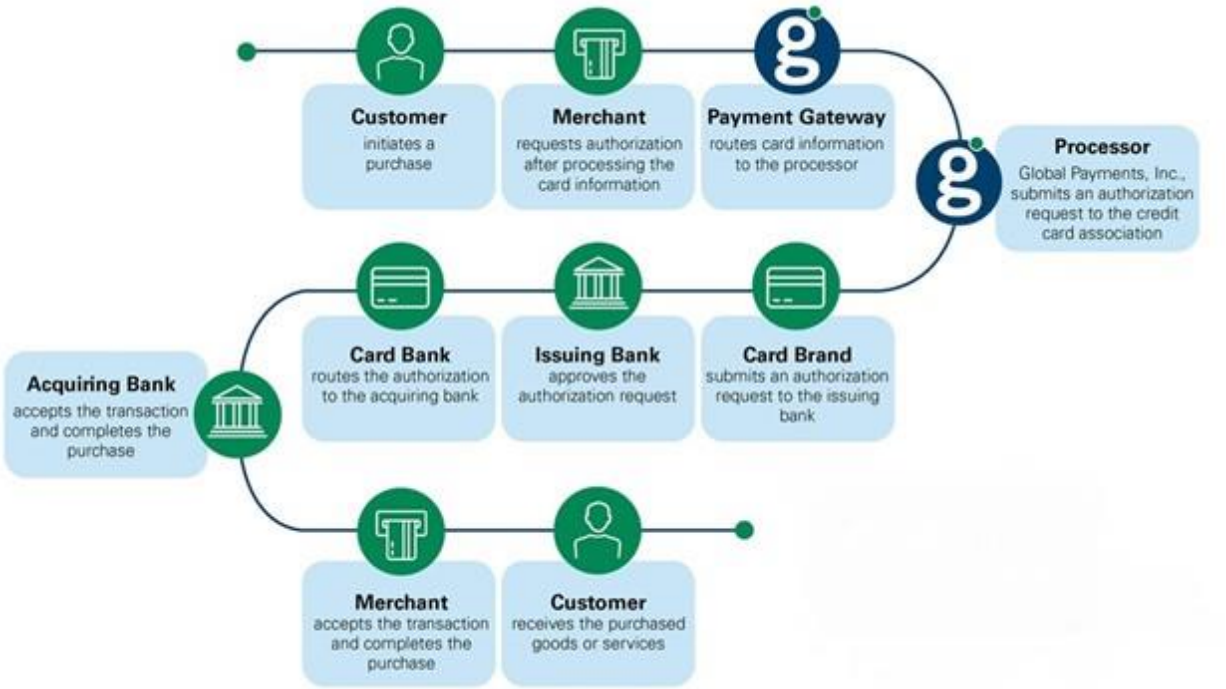
From here, the Acquiring Bank forwards the authorization to the Merchant's POS terminal, which then collects and processes all approved transactions.

9. The Merchant accepts the transaction and completes the purchase

The transaction is accepted by the Participant and the Constituent's purchase can be completed.

10. The Cardholder receives the purchased goods or services

Finally, the Cardholder receives their goods or services. Within the next month, the Cardholder will receive the bill from their credit card Issuer for any purchases they have made or see the debit on their account.



2a: ***How does a Merchant get funded?***

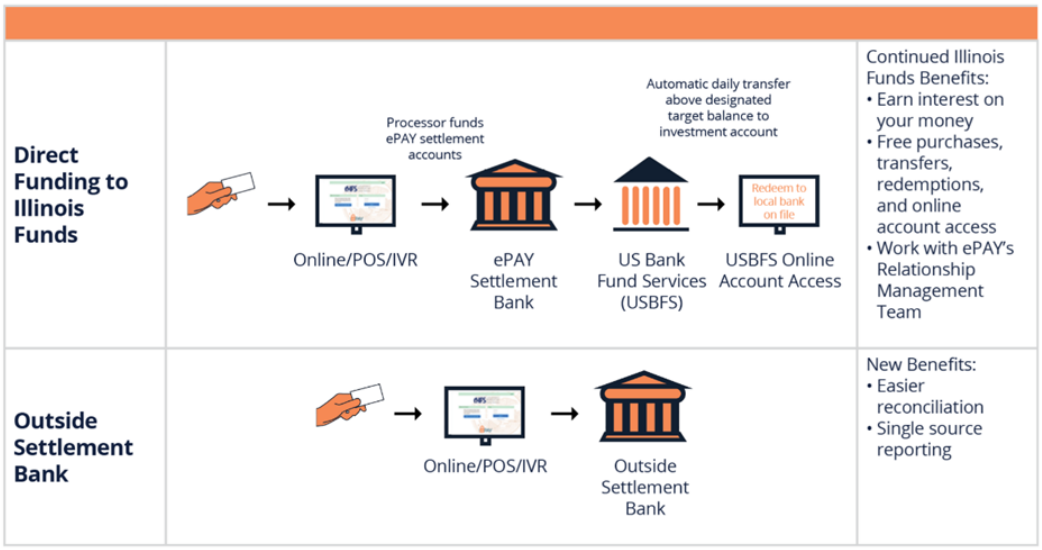
Credit Cards are funded to the Merchant's depositing bank on a 24-hour (1 Business Day) funding cycle depending on the Merchant's depositing bank rules for making funds available. eChecks are funded on a 24-hour (1 Business Day) funding cycle as well.

Should a Merchant decide to take advantage of the benefits of funding through Illinois National Bank (INB), there is typically an additional day delay in the Credit Card Funding Process. See more information below or visit the "New Participant" page on the IL State Treasurer ePAY Website, using the link below, for more information on the benefits of funding through IL National Bank.

https://illinoistreasurer.gov/Local_Governments/New_Participant

With ePAY, government agencies have the opportunity to earn greater returns as part of The Illinois Funds, an AAA rated fund recognized for its safety, liquidity, and return capabilities. ePAY funds are swept directly into your Illinois Funds investment account(s)[1], or you can elect to fund to a settlement account at a bank of your choosing.[2]

How it works



[1]Illinois National Bank (INB) is the custodian for ePAY settlement account(s). INB automatically transfers any funds over your target balance to your Illinois Funds investment account(s) at US Bank at 8:30 a.m. daily.
[2]Unless a state agency has the option to fund to a locally held account.

Benefits with The Illinois Funds:

	Direct funding to The Illinois Funds	Outside Settlement
Monthly Maintenance Fee	$0*	Varies by Bank
Credit Fee	$0.10 per credit	Varies by Bank
Settlement Account Earnings Credit Rate	0.17% APY	Varies by Bank
Online Banking	1 user free ($5 per additional user)	Varies by Bank
Minimum Target Balance	$1,000-$250,000	Varies by Bank
Fee for Insufficient Funds	$30	Varies by Bank
Interest Earnings	Yes	None
Fees for Transfers	$0**	None
Funding/Settlement Customer Service Support	Assistance from ePAY Relationship Management Team	None

[1]Illinois National Bank (INB) is the custodian for ePAY settlement account(s) that fund to The Illinois Funds. INB automatically transfers any funds over your target balance to your Illinois Funds investment account(s) at US Bank at 8:30 a.m. daily. [2]State agencies do not have this option available per the Deposit of Statement Monies Act (15ILCS520), unless a state agency has the option to fund to a locally held account.
***ePAY processor will credit the Participant $10 every month to offset Settlement Bank account maintenance fees. **No fee for daily transfers from Illinois National Bank to Illinois Funds investment accounts at US Bank Fund Services. No fee for ACH or wire transfers from Illinois Funds investment accounts to banks on file.**

2b: **Retention of Sales Drafts**

An often overlooked and very important part of accepting payments is the retention of sales drafts. Whether a Merchant is accepting payments using a desktop POS device or with a semi-integrated POS terminal, Merchants should adhere to the retention process that will safeguard Cardholder Data.

The Merchant must safeguard all stored sales drafts and other transaction data that contain full card numbers (i.e., reports, screen prints) and provide limited (and only authorized) access to these items. Global Payments has applications that truncate both copies of the transaction receipt and only display the last four digits of the card number.

The Merchant must keep all systems and media containing Cardholder, account, or transaction information (whether physical or electronic) in a restricted, secure manner to prevent access by or disclosure to any unauthorized party. At the end of the 18-month retention period, the Merchant must render unreadable all transaction data, such as sales drafts, reports, and other media with Cardholder account data, prior to discarding it. If the Merchant has used a PC to access transaction information, then the PC must not be disposed of until information has been rendered unreadable.

The Merchant should always keep complete records for all payment card transactions in the event of chargeback requests. Do not store sales drafts in alphabetical order by customer. It is recommended that a Merchant storage system be one that is sorted chronologically by date and then by Cardholder account number.

Visa: Sales slip retention time frame is the "Life Cycle" of the transaction, and 120 days after the processing date. (NOTE: A best practice for chargebacks is to save transaction data or proof of purchase at least 180 days after services/product is provided.)

MasterCard: Sales slip retention time frame is 13 months.

Discover: Sales slip retention time frame is one (1) year from the Transaction Date, or two (2) years from the Transaction Date if the Transaction was subject to Dispute or as required by Applicable Law.

American Express: Sales slip retention time frame for Charge Records is twenty-four (24) months from the date Merchant submitted the corresponding Charge to American Express.

NOTE: ePAY Participant Merchants can access historical transaction data through the secure ePAY Dashboard reporting tool. All retention requirements above for all the Card Brands are adhered to by ePAY and Global Payments.

2c: Charging a *Service Fee*

ePAY Participants can choose to pass a fee (Passing) onto the Constituent when a credit card is accepted, or they can choose to absorb (Absorbing) that cost of processing a credit card.

Visa and the other Card Brands allow ePAY Participants to charge a service fee to Constituents when accepting payments and ePAY makes it simple by including the cost of accepting payments in two Passing Rate options when accepting credit cards. Global Payments and ePAY follow all rules and regulations and adhere to Card Brand Rules for charging a Service Fee. For more information, we have included a link to the latest version of Visa's Core Rules from April 2024. For more information on Service Fees, visit pages 379 – 388 in the doc link below for general guidance.

Visa Core Rules and Visa Product and Service Rules 5.5 Surcharges, Convenience Fees, and Service Fees April 13, 2024

Passing

Passing allows you to pass on the processing fees to your constituent. In addition, all passing pricing includes the cost of the POS equipment. The only decision you are asked to make is whether you will fund your Illinois Funds investment account or go outside and use your own settlement bank.

Learn more about Illinois Funds investment accounts here: https://illinoistreasurer.gov/Local_Governments/The_Illinois_Funds

Credit Card Processing Fees

	Processing Fee
Use ePAY's Settlement Bank*	2.25% minimum of $1.00
Use Participant's own Settlement Bank**	2.30% minimum of $1.00

*Contractor will credit the Participant $10 every month to offset monthly Settlement Bank account maintenance fees. **Processing Fee includes the cost of any Supported Device, selected by the participant, which shall be provided based upon Participant volume: $1 = 1 Supported Device per $300,000 in processing volume. Notwithstanding the foregoing, the Contractor reserve the right to offer Participants free supported Devices, regardless of processing volume.

Absorbing

Should a Participant decide to absorb the cost of accepting credit cards, the credit card processing fee structure below would apply.

Under absorb pricing you have the option to automatically deposit your funds into your Illinois Funds investment account or to your own settlement bank for higher pricing. Also, you have the option to include the cost of your POS equipment within your processing fees or pay for your equipment upfront.

Please note under this scenario the ePAY processor will auto debit your settlement account on the fifth day of the subsequent month or the next business day if the fifth day is a weekend or a holiday. However, state agencies will be invoiced by the fifth day of the subsequent month with payment due at fifty (50) days of receipt of an invoice.

Learn more about Illinois Funds investment accounts here: https://illinoistreasurer.gov/Local_Governments/The_Illinois_Funds

Credit Card Processing Fees

	Fees with no Supported Device (Participant purchases or rents)	Fees with Supported Device***
Use ePAY's Settlement Bank*	Cost^ plus 3 basis points and $0.03 per transaction	Cost^ plus 8 basis points and $0.03 per transaction
Use Participant's own Settlement Bank**	Cost^ plus 3 basis points and $0.03 per transaction. $15/mos.	Cost^ plus 8 basis points and $0.03 per transaction. $15/mos.

*Contractor will credit the Participant $10 every month to offset monthly Settlement Bank account maintenance fees. **Contractor will assess the Participant $15 every month regardless of the number of accounts held by such Participant. ^Interchange rates, dues, assessments, and other pass through fees from the Card Brands or third party gateways.

2d: How long does a credit card payment take to process?

Payment verification only takes a few seconds at the point of sale or online. Then, the payment process continues behind the scenes with the settlement process.

1. Merchants send all approved transactions to the Acquirer at the end of the day. This group of transactions is called a batch.
2. The Payment Processor routes the batch to the Card Brand for settlement.
3. The Card Brand forwards the transactions to the Issuer.
4. The Issuer transfers the funds to the Acquirer, and in the process, takes an Interchange Fee. Card Brands set the Interchange Fee, and the Acquirer is responsible for paying this fee to the Issuer.
5. The Acquirer credits the Merchant's account with the approved transactions. Funding times to the Merchant vary, however, on average it takes one to three days. Additionally, batches sent during the weekend, or a bank holiday get processed on the next business day.
6. The Issuer posts the transaction on the Cardholder's account. The Cardholder will be responsible for settling their debt at the end of their billing cycle.

Learn more about how Credit Card Processing works by clicking the link below:

(YouTube Video Link) ☞ https://youtu.be/8RyEcMcuTxU

2e: Processing a refund

Generally speaking, when a Cardholder is requesting money back and the Merchant has agreed to refund a portion of or all of the original charge, the Merchant will generally credit the refund to the original form of payment. If the original payment was paid by a credit card, the Cardholder will not receive physical cash back. The Credit Card Issuer will post a statement credit to the Cardholder's account when the refund is processed, effectively reducing the Cardholder's statement balance by the refunded amount.

Examples of refunded transactions:

1. Cardholder paid by credit card one week ago and is requesting a full refund. The Merchant has agreed to the refund and a full credit of the original charge is submitted by the Merchant. The Cardholder receives a credit back to their credit card account for the full amount.

2. Cardholder paid by credit card 2 days ago and is requesting a partial refund. The Merchant has agreed to the refund and a partial credit of the original charge is submitted by the Merchant. The Cardholder receives a partial credit back to their credit card account for the agreed amount.

3. An Individual provides their bank account information online to pay for services from a Merchant. Two days later, the individual realizes they purchased the incorrect service and contacts the Merchant for a full refund. The Merchant agrees and credits back the Individual using their securely stored bank account information.

Refunds should not be confused with Voids. A transaction can only be voided when the transaction has yet to be settled for the day. A refund is only done after the original purchase has been settled and transferred to the Merchant's bank. The settlement occurs typically every day at the end of business and all payments accepted by a Merchant are settled and sent to their bank for deposit. This is formally known as the "Settlement Process" or "Batch Process."

2f: What happens when a credit card transaction gets declined?

A declined credit card transaction can be caused by many factors including, and not limited to, the following:

1. Insufficient funds.

2. Incorrect credit card information.

3. International charges.

4. Technical issues experienced by the credit card company or Issuing Bank.

5. Fraud prevention measures (i.e., A customer makes multiple purchases that seem unusual.)

Should a credit card be declined, it is acceptable to process the transaction one more time to exclude any physical reasons for decline. After two separate declined transactions, it is advisable to ask the Cardholder for another form of payment.

2g: Prohibited Transactions

Merchants who accept credit cards must be aware of Prohibited Transactions and the penalties that can be imposed if they complete them. A Prohibited Transaction is one that does not comply with the operating regulations of the Visa, MasterCard, American Express and Discover associations and/or policies and procedures as defined in the Merchant Agreement. If deposited, sale drafts involving Prohibited Transactions will be subject to a chargeback and may lead to termination of the Merchant Agreement.

Merchants must educate their staff about Prohibited Transactions to reduce the risk of accepting Counterfeit Transactions or Fraudulent Transactions. A Fraudulent Transaction could involve an invalid account number, or a valid number with unauthorized use. Unauthorized use of a lost or stolen card is one of the greatest contributors to fraud losses. In the case of stolen cards, fraud normally occurs within hours of the loss or theft – before most victims have called to report the loss.

Examples of Prohibited Transactions

1. Processing transactions to cover previously incurred debts, or bad debts, such as bounced checks, or payment for returned merchandise. Visa permits this practice if the existing debt transactions are identified properly, and the account is not in collection.

2. Processing a sale on a previously charged back transaction.

3. Accepting transactions that are declined by the Voice Authorization.

4. Attempting multiple authorization requests following a decline.

5. Accepting cards with an invalid effective date.

6. Accepting expired cards.

7. Using a split sale to avoid authorization requirements.

8. Giving cash to the Cardholder unless set up for cash back.

9. Delivering goods or performing services after notice of a cancellation by the Cardholder of a pre-authorized order.

10. Billing card after notice of cancellation of recurring payment.

11. Accepting transactions where the signature on the card and the one on the sales draft are not the same.

12. Engaging in factoring (draft laundering} or accepting or depositing drafts from other banks, Merchants, or businesses which the Merchant may own or purchase and are not explicitly listed in the current Merchant Agreement (or supplements to it) currently on file with Global Payments. Laundering of deposit drafts will likely result in the immediate termination of the Merchant's bankcard privileges.

13. Depositing a sales draft twice.

14. Depositing a sales draft in one or more financial institutions for payment before or after it is deposited with Global Payments.

Now that you have been introduced to the basics of credit card acceptance, the next section will discuss the importance of following basic security rules as laid out by the Payment Card Industry.

Section 3: Credit Card Transactions and PCI-DSS Compliance

3a: What is PCI-DSS?

PCI-DSS stands for Payment Card Industry Data Security Standard. The standard is developed by the PCI Security Standards Council, which was formed in 2006.

The PCI-DSS sets forth the minimum-security features that must be in place to limit the chances of a Cardholder Data compromise. Merchants that comply with the PCI-DSS are less likely to suffer a breach event.

All entities that store, process or transmit Cardholder Data must validate PCI-DSS compliance. Merchants should work directly with their Acquiring Bank for instructions on how to validate PCI Compliance.

With every credit card transaction that takes place, it is important that the Cardholder's sensitive information is protected. This means that all products must be PCI Compliant. This ensures the security of credit card transactions.

The PCI Data Security Standards for the payment card industry are the minimum criteria Participants should strive for in order to avoid data breaches. There are 12 PCI DSS requirements, which detail proper methods for storing credit card numbers and beyond. PCI DSS is the data security standard for the payment card industry and is maintained by the PCI Security Standards Council (PCI SSC).

Read on to learn the 12 requirements of PCI DSS, what they entail, and how you can stay PCI Compliant. ***By being an ePAY Participant, you will receive assistance with completing your annual PCI Compliance.***

3b: The PCI Data Security Standard

There are six major principles of PCI DSS.

Think of these principles as the “goals” that the various PCI DSS policies and procedures intend to achieve.

All 12 requirements pertain to a principle, and these principles are:

1. Build and maintain a secure network.
2. Protect Cardholder Data.
3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Regularly monitor and test networks.
6. Maintain an information security policy.

If these conditions are met, then the Payment Card Transaction Environment is compliant.

3c: The 12 Requirements of PCI DSS

The requirements set forth by the PCI DSS are both operational and technical, and the core focus of these rules is to protect Cardholder Data at all times.

These standards apply not just to Merchants but anyone that stores, processes, transmits, or otherwise manipulates Cardholder Data. Service providers who can affect the security of Cardholder Data are also responsible for compliance with applicable requirements. PCI DSS applies for mobile applications as well, so it is important to have a solid understanding of the standards.

The 12 requirements of PCI DSS are:

1. Install and maintain a firewall configuration to protect Cardholder Data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored Cardholder data.
4. Encrypt transmission of Cardholder Data across open, public networks.
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to Cardholder Data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to Cardholder Data.
10. Track and monitor all access to network resources and Cardholder Data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

1. Install and maintain a firewall configuration to protect Cardholder Data

Criminals no longer need physical access to Cardholder Data in order to steal it, and a core PCI DSS goal is to build and maintain a secure network.

This first requirement ensures that Merchants do so through the proper configuration of a firewall as well as routers if applicable.

Organizations should establish firewall and router standards, which allow for standardized testing of that equipment whenever hardware or software changes are made. Configuration rules should be reviewed biannually and should restrict all untrusted traffic except in cases where that communication protocol is required to process Cardholder Data.

It is necessary to prohibit access from the internet to any component within the Cardholder Data environment. If employees or other relevant personnel have computers or mobile devices that access the organization's network, those systems must be equipped with personal firewall software.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Among the most common and simplest exploits available to criminals is the ability to compromise a system because a firewall, router, or other hardware or software uses a standard password. Routers, for instance, often ship with the username "admin" and the password "admin" for the sake of convenience.

Such default passwords and other security parameters are not permissible per this requirement. Those parameters must be changed before the new item interfaces with the established system in any way.

3. Protect stored Cardholder Data

Any organization that accepts payment cards is required to protect Cardholder Data in order to prevent unauthorized usage. Cardholder Data should never be stored unless required for legal, regulatory, or business needs. In the event storage is necessary, this requirement focuses on securing stored data.

Organizations must limit storage and retention time to the bare minimum and should perform a purge at least every quarter. Sensitive data, even if encrypted, should never be stored beyond what is necessary to finalize a transaction.

This requirement also includes rules for how primary account numbers should be displayed, such as revealing only the first six and last four digits. This requirement does not supersede other legal or payment Card Brand requirements, including requirements that further limit data which can be displayed on point-of-sale (POS) receipts.

4. Encrypt transmission of Cardholder Data across open, public networks

Cyber Criminals can potentially access Cardholder Data when it is transmitted across public networks. Encrypting that data prior to transmitting it and then decrypting it upon receipt limits the likelihood that thieves can access this data in a meaningful way.

This requirement demands strong cryptography and security protocols. It also provides recommendations to protect Cardholder Data during transmission, such as IPSec, SSH, and TLS, and necessitates employing the latest industry standards, such as IEEE 802.11i for wireless networks.

5. Use and regularly update anti-virus software or programs

PCI DSS necessitates a proactive and ongoing approach to discovering weakness within a payment card system. This is referred to as a Vulnerability Management Program, and this first rule toward that end requires the deployment of an anti-virus solution. Such software must not just be used on core systems. Many vulnerabilities originate via email and other seemingly innocuous online activities.

Anti-virus software should be deployed on all systems, including the workstations, laptops, and mobile devices that employees may use to access the system both locally and remotely. Ensure that anti-virus mechanisms are always active, using the latest dictionaries, and generating auditable logs.

6. Develop and maintain secure systems and applications

Continuing on with managing vulnerabilities, organizations must limit the potential for exploits by keeping software secure. In many cases, this involves installing security patches as soon as available, and organizations must work to ensure that are instituting security patches, when necessary, and can access and execute them easily.

In addition to deploying critical patches in a timely manner, organizations must have a process in place not only to discover new vulnerabilities but also to rank them. All code created must be in accordance with PCI DSS, and all new code and changed code must be analyzed for all known vulnerabilities and also assessed for unknown weaknesses that the new code may reveal.

7. Restrict access to Cardholder Data by business need to know

In order to implement strong access control measures, Merchants must be able to allow or deny access to Cardholder Data as requested. The goal is to allow only authorized access, and unauthorized access is not simply limited to criminals. A person or an organization may request data that it does not need within the context of the current task; that request would be unauthorized and thus denied.

Need to know is a fundamental concept within PCI DSS. An agent may have permission to access certain data in a broad sense but not within a particular scenario. Therefore, an access control system must assess each request not just based on the agent making the request but also the circumstances. It must then deny any request that is not specifically permitted.

8. Assign a unique ID to each person with computer access

Having strong control measures in place requires that every authorized user have a unique identifier assigned to them. This ensures that whenever someone accesses Cardholder Data, that activity can be traced to a known user or at least immediately recognized as unauthorized access.

For remote access, Two-Factor Authorization is required. You cannot use one factor twice. Even the use of two distinct passwords is not advisable. PCI DSS recommends technologies like RADIUS and TACACS, which use tokens – meaning you have a password as one factor and a token as another.

9. Restrict physical access to Cardholder Data

Another aspect of implementing control measures involves limiting the physical access that parties may have to this sensitive data. These parties can include employees, contractors, vendors, consultants, and guests, and access includes any opportunities to retrieve data via systems, devices, and hard copies.

Such protection requires on-site access control that not only restricts movement within an installation but also monitors and logs it. There must be procedures in place to easily and quickly identify people who do not belong, and a site requires security personnel dedicated to enforcing these rules.

All media must be physically secured, and backups should be maintained at a site other than the primary location. Additionally, there must be procedures and controls in place to determine how information is distributed so that data does not become exposed after access has been approved.

Finally, it is necessary to destroy all media when the business no longer needs it, or a legal obligation may present itself.

10. Track and monitor all access to network resources and Cardholder Data

Cardholder access points are connected via both physical and wireless networks, and vulnerabilities in these networks make it easier for criminals to steal data. PCI DSS aims to prevent these exploits by requiring organizations to monitor and test their networks on a regular basis.

This requires real-time monitoring and logging as well as forensic mechanisms. But in order to make these systems effective, a certain foundation is required. This particular requirement focuses on those underpinnings, such as the ability to link all network traffic to a specific user.

Automated audit trails are necessary as well as the ability to reconstruct events. Audit trail records must meet a certain standard in terms of the information contained. Time synchronization is required. Audit data must be secured, and such data must be maintained for a period no shorter than a year.

11. Regularly test security systems and processes

Vulnerabilities are introduced recurrently not just by criminals but by researchers and through the introduction of new code. This means that all systems and processes must be tested on a frequent basis to ensure that security is maintained despite these environmental changes.

Organizations must test each quarter for wireless access points used to gain unauthorized access. Internal and external vulnerability scans are required at least every quarter but also whenever a significant network change has been made. Other ongoing requirements include penetration testing as well as the use of intrusion detection and prevention systems.

File monitoring is a necessity, too. This mechanism can raise an alert whenever a user has modified a content, configuration, or system file in an unauthorized manner. The system should perform file comparisons each week to detect changes that may have otherwise gone unnoticed.

12. Maintain a policy that addresses information security for all personnel

This final requirement is dedicated to the core PCI DSS goal of implementing and maintaining an information security policy for all employees and other relevant parties. It is necessary not just to create and maintain the policy but also to publish and disseminate it.

There must be at least a yearly process through which the policy is challenged and then revised as required. It is also necessary to ensure that all security procedures and usage policies are in accordance with the primary information security policy.

The requirement demands that there be at least one agent (and perhaps an entire team depending on the scope) who is responsible for these obligations. These personnel oversee the creation of awareness campaigns relevant to information security and are required to screen prospective employees, contractors, and so forth as part of the hiring process to avoid internal data breaches.

3d: What Is Cardholder Data?

Cybercriminals are looking to steal account data by compromising Merchants and Merchant Service Providers. This data is classified as either Cardholder Data (CHD) or Sensitive Authentication Data (SAD).

Cardholder Data (CHD) is typically data that is printed on the front of the card. This includes the primary account number (PAN), Cardholder name, and expiration date. Sensitive Authentication Data includes the CVV code, track data contained in the magnetic stripe, PIN/PIN Block, and EMV chip data.

3e: What Cardholder Data Can and Cannot Be Stored

Sensitive Authentication Data cannot be stored after authorization. Storage of Cardholder data must be limited to that which is required by legal, regulatory, or business needs.

3f: PCI Data Storage: Do's

Do: Know the flow of Payment Card Data throughout the transaction process.

Merchants and Merchant Service Providers must be aware of the flow of account data throughout the transaction process. Merchants are responsible for developing data retention policies and understanding which systems may affect the security of account data.

Do: Use strong cryptography to render unreadable Cardholder Data that is stored.

If Cardholder Data is stored, it must be rendered unreadable using one of the accepted methods listed in PCI-DSS required 3.4. This must be done through either one-way hashes, truncation, index tokens and pads, or strong cryptography including requirements for key management and strength at or above industry standards.

Use industry-tested and accepted hashing algorithms for encryption including SHA-1, AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher) along with layered security technologies to minimize the risk of data compromise. Additionally, Merchants must have a methodology for secure deletion and a quarterly process to identify the presence of Cardholder Data stored outside of the retention policy.

Do: Follow PCI DSS requirements, validated by yourself or outside assessment.

All Merchants and Merchant Service Providers involved in the storage, processing, and transmission of account data must validate PCI Compliance. The PCI-DSS is a list of requirements designed to limit the possibility of exposure of account data. This exposure is typically the result of malicious actors looking to compromise Merchants through physical means, or more commonly, through the use of malware. Small Merchants can validate PCI Compliance through a self-assessment questionnaire, or SAQ, process. Larger Merchants and service providers should engage a third-party Qualified Security Assessor to validate compliance with all PCI requirements.

Do: Be sure to report regularly as a part of mandated PCI DSS compliance.

Merchants are required to validate compliance annually. Merchants should submit evidence of compliance to their Acquiring Bank in accordance with that Acquiring Bank's PCI Compliance Program.

Do: Ensure third parties who process customers' payment cards comply with the PCI DSS as applicable.

Merchants are always responsible for the security of their customers' account data. In cases where a Merchant has engaged with a third party that can affect the security of that data, they must validate the PCI compliance of those entities. If a third-party service provider has not validated PCI Compliance, the

services provided must be validated as part of the Merchant's PCI validation. A service provider must provide the Merchant with clear access and password protection policies.

PCI Data Storage: Don'ts

Don't: Store Cardholder Data unless necessary.

Merchants can never store sensitive Authentication Data after authorization. Merchants can store Cardholder Data and should only do so when absolutely necessary for legal, regulatory or business purposes. Stored Cardholder Data is a target for cybercriminals looking to steal this data and use it to perform fraudulent transactions. For card-on-file or recurring billing transactions, Merchants should take advantage of tokenization services.

Don't: Store sensitive Authentication Data contained in the payment card's chip or magnetic stripe.

Data contained in the EMV chip and magnetic stripe, as well as the three- or four-digit validation code (CVV) and PIN/PIN Block, are considered sensitive Authentication Data and cannot be stored.

Don't: Print or display Cardholder Data that is not adequately masked.

Merchants must not print the expiration date or unmasked primary account number on receipts. The primary account number should be masked whenever printed or displayed, with the maximum number of digits being the first six and last four digits.

Don't: Store Payment Card Data in unprotected endpoint devices or send data through chat, messaging, or other end-user messaging services.

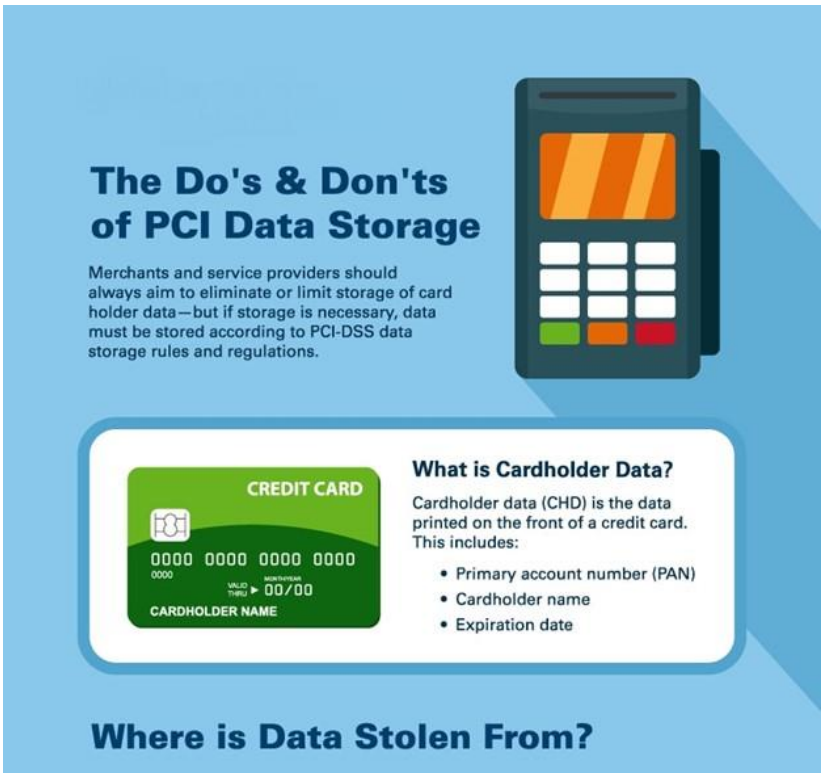
Cardholder Data must only be stored in a secure environment that is not accessible to the public internet. This data cannot be stored on unprotected endpoint devices such as a phone, laptop, or PC. This data must also not be sent through chat, messaging, or other end-user messaging services.

Don't: Locate servers/payment card system storage devices outside of fully secured rooms.

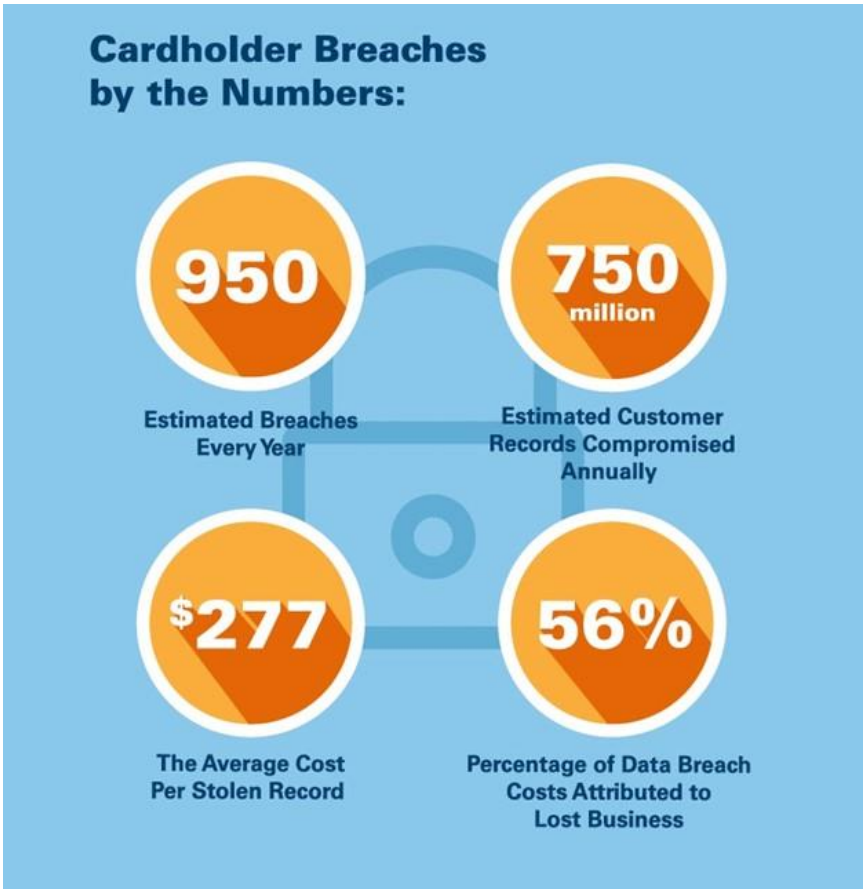
Access to any systems that store Cardholder Data must be restricted appropriately. This includes access control measures that include visitor logs, physical access controls and video monitoring. Databases that store Cardholder Data cannot be available to the public internet.

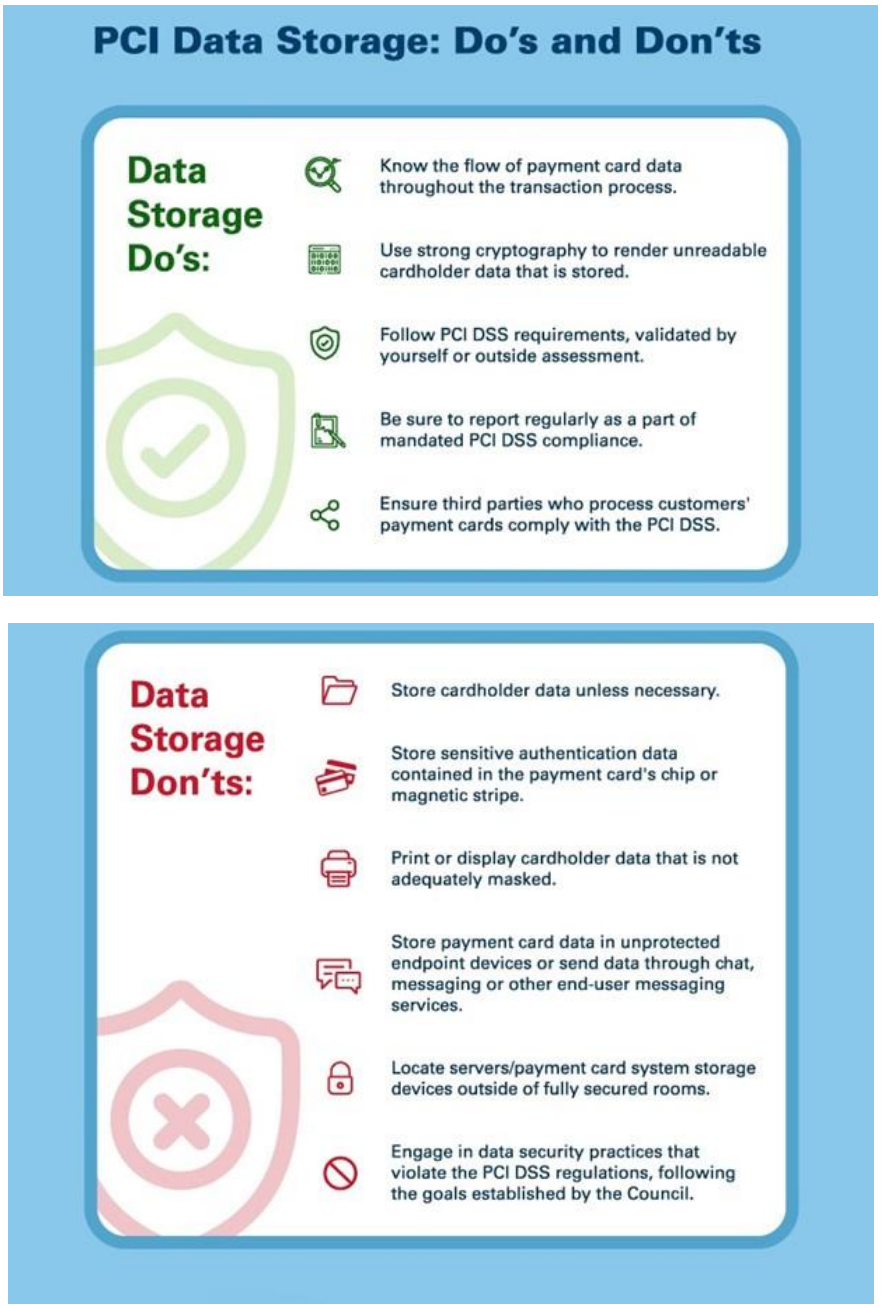
Don’t: Engage in data security practices that violate the PCI DSS regulations, following the goals established by the Council.

Merchants that fail to comply with the PCI-DSS requirements are much more likely to become a victim of a data breach. Validating PCI compliance and developing robust policies and procedures to protect or eliminate stored Cardholder Data is the best way to avoid a costly data breach.




Card Readers
Payment System Database
Wireless or Wired Networks
Paper Records


Cardholder Breaches by the Numbers:
950
Estimated Breaches Every Year
750 million
Estimated Customer Records Compromised Annually
$277
The Average Cost Per Stolen Record
56%
Percentage of Data Breach Costs Attributed to Lost Business



Section 4: What is a credit card chargeback?

Credit Card Chargebacks are unavoidable for businesses that accept credit cards. While chargebacks only happen to a small percentage of transactions, it is still something Participants need to keep an eye on to reduce losses.

A credit card chargeback is not the same as a refund. When a constituent is dissatisfied with a product or service, they can directly approach the state agency or local municipality, choosing to request a refund for the product or service and asking for their money back.

For State Agencies or Municipalities, this can be a straightforward process. If they decide to process the refund, the funds will return to the Constituents credit card in a short amount of time.

However, some Cardholders may choose to dispute the charge with their credit card company (their Issuing Bank) rather than directly contacting the Merchant. When they initiate a credit card chargeback, they send the transaction back to the Merchant's bank (or Acquirer). The Issuing Bank requests the Acquirer to take away the disputed funds and credit it back to the Cardholder.

The Acquirer then has to contact the Merchant, asking if they would like to challenge the claim. Response times vary, and if the Merchant chooses to respond, this will lengthen the timeline for resolution.

The following video explains the chargeback process in more detail:

(YouTube Video Link) ☞ https://www.youtube.com/watch?v=PvbBDnWs-3U

4a: Types of Chargebacks

There are generally three different types of chargebacks.

1. "C*riminal (True) Fraud*" Scammers steal the Cardholder's identity. In this case, the Merchant should not attempt to dispute this type of chargeback.

2. "*Chargeback Fraud*" – The transaction is valid, but the Cardholder has buyer's remorse or simply wants to get free items. In their dispute, they may claim that they didn't authorize the transaction.

3. "*Friendly Fraud*" – The Cardholder issues a chargeback due to an honest mistake. There may be some errant data or description of services that does not match what the Cardholder purchased, or the Cardholder simply does not recognize the transaction. Rather than issuing an inquiry into the source of the transaction in the form of a retrieval request, the Cardholder issues a chargeback.

4b: Dos and Don'ts

Dos

1. Do choose a reputable payment processor: Make sure to research and choose a payment processor that is reliable, secure, and has a good reputation in the industry.

2. Do encrypt sensitive data: Use encryption technologies to protect sensitive data such as credit card numbers and personal information.

3. Do have a clear and transparent pricing structure: Ensure that your customers are aware of any fees associated with their transactions and that they understand how these fees are calculated.

4. Do monitor for fraud: Use fraud detection and prevention tools to protect yourself and your customers from fraudulent transactions.

5. Do provide excellent customer service: Make sure your customers have access to help and support if they have any issues with their payments or transaction

Don’ts

1. Don’t store sensitive data: Avoid storing sensitive data such as credit card numbers and personal information unless it is absolutely necessary.

2. Don’t use unsecured networks: Avoid using public or unsecured networks when processing payments as these can be vulnerable to hacking and other security risks.

3. Don’t ignore chargebacks: Chargebacks occur when a customer disputes a charge on their credit card. Make sure to respond to chargebacks promptly and provide any necessary evidence to support your case.

4. Don’t neglect compliance requirements: Ensure that you are complying with industry regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS) to protect your business and your customers.

5. Don’t overlook user experience: Ensure that your payment processing system is easy to use and provides a smooth and seamless user experience for your customers. Difficult or confusing payment processes can lead to abandoned transactions and lost sales.

4c: Why are credit card chargebacks bad for business?

The chargeback process costs Participants money in the form of Chargeback Fees. Unfortunately, these fees can apply regardless of whether the Participant wins the arbitration process. Industry Retrieval Request Fees generally range from $5.00 to $20.00. Chargeback fees vary per payment processor, ranging from $5 to $100 per incident.

If the dispute reaches the arbitration stage, the Card Brand can charge $250 to $500 in fees. The losing party is responsible for paying these fees.

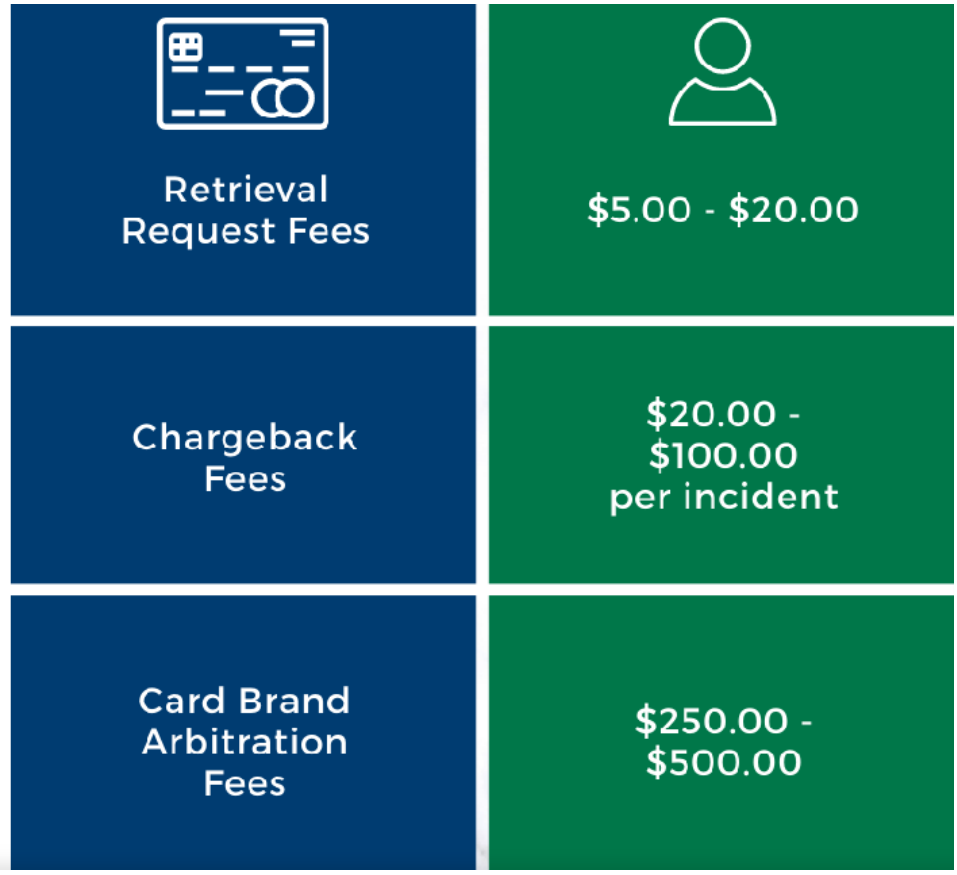
On top of the fees, the major Card Brands have strict limits – generally 1% of sales volume – that can trigger additional fines or account termination. Please see below the typical industry charges for Retrieval Requests and Chargeback Fees.

These fees for ePAY Participants are much lower than the industry norms.

ePAY Participant Fees

Chargeback and Return Fees	Fee
Chargeback fee when EMV device utilized	$5.00 per chargeback, fee paid by Participant
Chargeback fee when non-EMV device utilized (includes Web/IVR)	$15.00 per chargeback, fee paid by Participant

Industry Norms



4d: How can businesses reduce chargeback fraud?

Providing excellent customer service, clear communication, training staff properly on accepting payments, and maintaining payment security standards are essential to keeping chargeback fraud to a minimum.

Communicate with Cardholders

Merchants can oftentimes avoid chargebacks through open, direct communication and following these simple steps:

1. Clearly describe offerings to Cardholder to avoid confusion.

2. Explain return, cancellation, and refund policies in detail, and keep it simple so customers do not feel like a chargeback is the only way to resolve the dispute.

3. Share what the customer can expect in terms of after-sales service.

4. For card-present or face-to-face sales, full return and refund policies should be on all receipt copies.

It is best to make full return and refund policies available on your website or application in card-not-present environments, in addition to a "Click to Accept" or other acknowledgment button, checkbox, or location for an Electronic Signature.

Use payment processing software that provides up-to-date security features

The software solutions that Merchants use for managing their business and processing payments should include the most up to date security features to ensure they are reducing the potential for fraud as best as possible. Some examples include:

1. EMV Quick Chip and EMV contactless - Cards with EMV chips are less susceptible to payment fraud, as it is difficult for fraudsters to skim and duplicate them. EMV-enabled hardware can also provide the documentation needed to defend your business when you submit your chargeback rebuttal.

2. Tokenization - Tokenization is a best practice that replaces Cardholder Data (CHD) such as credit card information with one or more unrelated symbols it generates randomly or by algorithm. Including this feature in a security bundle will help keep large volumes of transactions secure.

3. Encryption - Encryption is a process that encodes information so that it is unreadable unless decrypted by someone with knowledge of the decryption key. Including encryption as a security feature helps provide confidence that CHD is safe.

Actively monitor disputes

When Merchants receive a chargeback notification, they have an opportunity to respond and defend themselves. The Merchant should:

1. Follow all instructions in the chargeback notification.

2. Respond by the due date given.

3. Address all Cardholder concerns in writing.

4. Provide proper transaction documentation such as order forms, invoices, and more.

ePAY Participants can monitor all chargebacks and resolve issues quickly by responding to all emails that are sent by the Chargebacks Team with Global Payments. The Global Payments' Chargebacks Team automatically responds to all incoming Chargebacks and Retrieval Requests and informs the Participant with an email.

Section 5: Fraud Prevention

Apart from Chargeback Fraud that was discussed in the previous section, there are other types of fraud that are focused on the Cardholder and not the payment process. It is good practice to be familiar with the common types of fraud to protect yourself from being a victim.

5a: Common types of fraud

1. Phishing – The fraudster presents himself as a trusted entity and convinces the unsuspecting victim into clicking a malicious link. This allows the fraudster to secretly access the victim's sensitive information and often gain control of the victim's login credentials. The fraudster then takes control of the victim's accounts to make fraudulent purchases.

2. Buy-Online & Pickup – This is the second half of the Phishing Fraud. The fraudster uses stolen account information to purchase goods/services online and then picks up the goods/services in person before the Merchant can detect the fraud.

3. Refund Fraud (Return Fraud) – The fraudster purchases goods/services online and then visit the Merchant location to request a refund.

4. Card Testing (Tumbling) – A fraudster uses bots to conduct hundreds of small value transactions with stolen credit card numbers to determine which cards can be used for higher value fraudulent credit card transactions.

5b: Best Practices of how to prevent fraud

While not all of the below practices may make sense for your organization, implementing basic fraud prevention strategies can have a sizable impact in preventing fraudsters from accessing confidential information.

Some Best Practices

1. Use a verified payments partner and understand the methods and practices that your payments partner utilizes

2. Encrypt & Tokenize transactions

3. Regularly change your login credentials

4. Set policies for accessing confidential information

5. Restrict access to confidential information to only those necessary individuals

6. Require customers to setup accounts to make a purchase

7. Implement your own customized fraud management tools and strategies

The most important practice is to alert Global Payments and ePAY if you suspect you are a victim of fraud or have detected fraudulent activity.

Section 6: Card-Not-Present and eCommerce Transactions

6a: Completing Card-Not-Present and eCommerce Transactions

Card-Not-Present transactions are those that occur when there is no face-to-face contact with the Cardholder. These transactions typically include the following:

1. MOTO Transactions – Transactions by mail or telephone
2. By fax
3. Over the Internet (also referred to as eCommerce or Online Transactions)
4. Commercial cards and Purchase cards with line-item detail

Take precautions to guard against compromising data when taking orders over the Internet, by telephone, mail, or fax. Given that visual identification cannot be made for Cardholders requesting fax, mail, phone or electronic commerce transactions, some personal information must be obtained in order to receive authorization from Global Payments. When processing fax, telephone, mail or electronic commerce transactions, Merchants should always remain aware of the increased risk of fraud because the Cardholder is not present.

NOTE: We HIGHLY discourage accepting payment through any method other than directly through an Encrypted POS Device, through a secure Online Portal, or an IVR Payment System. These secure methods will keep your PCI Compliance process in check and also will protect Cardholder Data.

Global Payments offers multiple methods of accepting payments online through the ePAY Dashboard. Participants can integrate their website and accept payments in a secure manner in a variety of ways. Participants can integrate to the ePAY Dashboard using a Fully Hosted, Re-Direct Integration or iFrame. Within the ePAY Dashboard, there are also features that allow Participants to send a link to Constituents to make a payment and also set up recurring payments for Cardholders.

6b: How do online payment methods stay secure?

The card payment industry has standards in place to protect Constituent's information should a security breach occur. The Payment Card Industry Data Security Standard (PCI-DSS) lays out the minimum-security features needed to limit the chances of compromised data.

Encryption is one way to protect Cardholder Data. As laws become more stringent over time, in addition to increasing cybersecurity threats, encryption uses a numeric binary code to shield sensitive data such as the Cardholder's name, account number, expiration date, and service code. The more random the encryption code is, the more difficult it is for hackers to gain access.

Tokenization is another way of protecting Cardholder Data, particularly the Cardholder's account number. During an online transmission, a token replaces the account number with a unique string of characters. Tokenization differs from encryption in that each token is original and can apply only to a specific Merchant and Cardholder.

Global Payments and ePAY use both Encryption and Tokenization to ensure that Cardholder Data is secure.

Section 7: Credit Card Machines

Today, there are various credit card machines available that can cater to any processing environment. Popular devices include **point-of-sale (POS)** terminals, which support credit cards with magnetic stripes and chips. Some are magnetic stripe ("magstripe") only, in addition to devices specially made for an unattended or kiosk type of environment.

Near-Field Communication (NFC) readers are payment terminals that allow tap-to-pay capabilities for contactless credit cards and mobile wallets.

Point-of-Sale (POS)

Simple and convenient over-the-counter payment solutions. Our recommended integration option is Hosted, Semi-Integrated because it offers real-time reporting capabilities, as well as the ability to utilize text or e-receipts.

Comparison of Integration Options: PAX POS Devices

	Option 1 (Preferred) Hosted Semi-Integrated	Option 2 3rd Party Hosted Semi-Integrated	Option 3 Stand-Alone to NCR Payment Solutions
Hardware Model	PAX A80 / A920* / Pax A35 (No Printer)	PAX A80 / A920* / A77**	PAX A80 / A920* / A77**
Process EMV Payments	✓/✓/✓/✓	✓/✓/✓/✓	✓/✓/✓/✓
End-to-end encryption to limit PCI Scope	✓/✓/✓/✓	✓/✓/✓/✓	✓/✓/✓/✓
Real time reporting capabilities through the ePAY Dashboard	✓/✓/✓/✓	✓/✓/✓/✓	X/X/X
Cashier reports from terminal	✓/✓/✓/✓	X/X/X	✓/✓/X
*Wireless & ethernet capable with purchase of separate base	**Wi-Fi capable only (No Printer)		

Point-of-Sale (POS)

Simple and convenient over-the-counter payment solutions. Our recommended integration option is hosted, semi-integrated because it offers real-time reporting capabilities, as well as the ability to utilize text or e-receipts.

Comparison of Integration Options: Verifone POS Devices

	Option 1 (Preferred) Hosted Semi-Integrated	Option 2 3rd Party Hosted Semi-Integrated	Option 3 Stand-Alone to NCR Payment Solutions
Hardware Model	Verifone V200c / Verifone V400c	Verifone V200c / Verifone V400c	Verifone V200c / Verifone V400c
Process EMV Payments	✓/✓	✓/✓	✓/✓
End-to-end encryption to limit PCI Scope	✓/✓	✓/✓	✓/✓
Real time reporting capabilities through the ePAY Dashboard	✓/✓	✓/✓	X/X
SMS text/e-receipt	✓/✓	✓/✓	✓/✓
Cashier reports from terminal	✓/✓	✓/✓	✓/✓
Verifone V400m*** Wireless POS Device	***Estimated availability Q1 2024		

Note: Hosted Semi-Integrated payment modes of collection support Customer account validation of account information. Account validation options may vary based on availability of data and Participant configurations.

(POS) Equipment Options

ePAY supports and recommends EMV point-of-sale (POS) transactions using the PAX and Verifone suite of POS devices offered. These specific devices were chosen to offer Ethernet, Wi-Fi, and Dial-Up connectivity. The PAX A80 offers (Ethernet or Wi-Fi connectivity) and the Verifone V200c offers (Ethernet, Wi-Fi connectivity and Dial-Up.) These EMV capable point-of-sale devices also offer Near-Field Communication (NFC) capabilities to allow for mobile wallet payments such as Apple Pay®, Google Pay™, and Samsung Pay®. The EMV readers also utilize point-to-point encryption (P2PE) to minimize PCI scope and protect card data. For a POS option where internet access and/or power is not available, the ePAY processor supports the PAX A920 and Verifone V400m for Wireless/Wi-Fi point-of-sale EMV payments, which utilizes the AT&T cellular data network. ePAY offers an Equipment Replacement Program on all equipment offered. Should your POS device(s) become defective at any time, while participating in the ePAY Program and processing transactions, your device will be replaced at no additional cost to you.*^**

^ Equipment Replacement Program excludes the CX5, CX7 and Aloha Silver POS Point-of-Sale solutions. These devices carry a separate warranty program.

To review the benefits of the Pax A77 click here.
To review the benefits of the Pax A80 click here.
To review the benefits of the Pax A920 click here.
To review the benefits of the Pax IM20 click here.
To review the benefits of the Pax A35 click here.
To review the benefits of the NCR-CX5 click here.
To review the benefits of the NCR-CX7 click here.
To review the benefits of the Pax Q25 click here.
To review the benefits of the Verifone P200 click here.
To review the benefits of the Verifone V200c click here.
To review the benefits of the Verifone V400c click here.

Section 8: What is Contactless Payment?

Recently, "contactless payment" has become the big buzzword across the payments landscape. But what does it actually mean, and how does it work? Learn the answers to these questions and more in our guide to contactless payments.

As defined by creditcards.com, contactless payments are "payment transactions that require no physical contact between the consumer's payment device and the physical terminal. To make this type of payment, the consumer holds the contactless card, device, or mobile phone close to the terminal and payment information is communicated wirelessly via radio frequencies."

Contactless payments, also sometimes referred to as "touchless payments," can be made one of two main ways: by a digital wallet or mobile app on a cellphone or other smart device, or by using a touchless payment card.

Digital Wallets/Mobile Apps

Digital wallets store a customer's payment information on a smart device such as a mobile phone, allowing customers to make payments without a physical credit card in hand. Some of the most popular digital wallets include Apple Pay®, Google Pay™, and Samsung Pay®.

Contactless Payment Cards

In addition to digital wallets, certain cards can also be used for touchless transactions. Rather than having to swipe the card as with magstripe cards, or dip the card as with chip cards, the consumer simply taps the payment card near a point-of-sale terminal that is equipped with contactless technology. For this reason, touchless payments are also often referred to with the phrases “tap to pay” or “tap and go.”

Other Payment Methods

Other payment methods that can also be considered touchless payments include card-on-file, where a business keeps a repeat customer’s card information so the customer does not have to present a physical card on each visit, as well as recurring payments, where a customer’s payment method is charged on a recurring basis, such as for subscription purchases.

Contactless Payment Symbol

EMVCo has established two main icons to refer to contactless payments – the contactless payment indicator and the contactless payment symbol. The indicator is depicted as four curved lines. When the indicator is shown on a payment card, it signals that the card can be used to make contactless payments. When it is shown on a card reader, it signals that the reader can be used to accept contactless payments.

The symbol shows the four curved lines and a hand holding a card, surrounded by an oval. It indicates where on the terminal the customer should tap their card or smartphone in order to make a contactless payment.

To view examples of the contactless payment indicator and symbol, visit the EMVCo website.

Which Technology is Predominately Used for Contactless Payment Systems?

Near-Field Communication, or NFC, is the technology used for touchless payments. NFC allows two devices in proximity to each other to communicate and share data, such as a digital wallet and a card reader. NFC technology is a more finely tuned version of radio frequency identification (RFID) technology.

Benefits of Contactless Payments

1. Security – Touchless payment cards and digital wallets are equipped with multiple security measures, including encryption of card data. Further security can be established by password-protecting any smartphone device that includes a digital wallet.

2. Efficiency – Touchless payments are fast and efficient, cutting down on transaction times and helping to make checkout lines move faster.

3. Versatility – Touchless payments allow businesses to diversify the payment methods they offer, giving customers a wider variety of payment options.

Is Contactless Payment Safe?

Contactless payment methods have surged in popularity recently, as they are considered a safer way to pay to avoid touching common surfaces. With only one person handling the payment method (smartphone or contactless card), these payment methods avoid the human contact that is involved with the exchange of cash or with handing a regular debit or credit card to a cashier.

From a security point of view, contactless payment methods are also considered safer than more traditional payment methods. Contactless cards use EMV technology, which is more secure than older magnetic stripe (magstripe) technology. Digital wallets use various security measures such as tokenization to protect Cardholder Data – and users can further protect their device by enabling the password protection feature.

Section 9: An Introduction to NFC

NFC, or Near-Field Communication, refers to technology that allows enabled devices that are near each other to wirelessly share data. Near-Field Communication has become an important part of the technology behind Mobile Payments. This guide will discuss what it is, how it works, and the benefits for integrating this technology into the solutions you offer.

What is NFC?

NFC stands for Near-Field Communication. This technology allows devices in close proximity to each other to easily communicate and share data. NFC has become a popular term in the payments industry in the last couple of years with an increase in contactless payments via mobile wallets. NFC payments have increased in popularity because they provide a quick and straightforward way for consumers to pay, saving them time at checkout.

You may have heard of "tap and go" payments, or even contactless payments – but how much do you know about the technology that powers this payment method? It is called Near-Field Communication, or NFC, and it allows two devices in close proximity to communicate with each other, such as when a smartphone or a wearable smart device communicates with a device at a cash register to process a payment.

NFC technology can be found in many smartphones, tablets, and wearables. It also powers many digital wallets, such as Apple Pay®, Google Pay™, and Samsung Pay®. NFC technology makes payments easier and quicker, as the purchaser can just tap or wave their smart device over the NFC-enabled payment device.

How Does NFC Work?

NFC technology evolved from radio frequency identification (RFID) technology. RFID can be used effectively at large distances, such as a pet microchip that can be scanned to identify a lost dog. NFC technology is more fine-tuned, operating at a range of about four inches or less. Chances are you have probably seen someone paying using their smartphone or smartwatch during checkout, and you may have noticed they had to wave their device near the payment terminal when paying via mobile wallet.

Data transmission via Near-Field Communication technology requires two NFC-enabled devices: a transmitting device and a receiving device. NFC technology works in one of two ways: one-way communication or two-way communication.

One-way communication: One-way communication requires an active NFC and a passive NFC device. An example of one-way communication is the interaction between an NFC-enabled smartphone being used for payment and a card reader.

Two-way communication: Two-way communication requires two active NFC devices. One example of this is the communication that occurs between two NFC-enabled smartphones during a file transfer.

The Technology Behind NFC

Radio-frequency identification, or RFID, is a technology that uses radio waves to relay identifying information from an electronic tag placed on an object to an electronic reader. RFID technology is used in pet microchips and access badges for office buildings and garages. NFC is a more fine-tuned subset of RFID, and is used to share data over smaller distances, such as in a contactless payment transaction.

NFC and Mobile

Near-Field Communication is the technology behind Mobile Payments. The wireless data transfer provided by Near-Field Communication technology enables contactless payments through mobile wallets such as Apple Pay®, Google Pay™, and Samsung Pay®.

NFC vs. Contactless

If you have heard the term "Contactless Payment" and then wondered what the difference between a Contactless Payment and NFC payment is, we are here to explain the two terms. A Contactless Payment is a secure way of paying that can use either NFC or RFID technology. Because NFC technology is what powers Contactless Payments, the terms are often used interchangeably. The term "contactless" tends to be used more generally and NFC tends to be used more specifically when speaking to the Near-Field Communication technology that is actually being utilized to process a payment.

NFC vs. EMV

While NFC and EMV are both secure ways of accepting payments, NFC refers to the wireless method of communication between two devices, whereas EMV refers to the technology that was originally created to replace magnetic stripe cards (or "magstripe" cards) with chip cards for more security.

EMV technology is a security feature that protects card Issuers, Merchants, and consumers from losses due to the use of counterfeit and stolen payment cards at the point-of-sale. EMV "smart cards" are embedded with a chip that interacts with a Merchant's point-of-sale device, ensuring the card is authentic and belongs to the user. This chip provides more security protection than magnetic stripe cards.

EMV can also be contactless, which is a method of payment that uses Near-Field Communication technology to complete a Mobile Payment.

Benefits of Offering Mobile Payment & NFC Functionality

The benefits of offering Mobile Payment and Near-Field Communication functionality to your clients are numerous. Below are just a few.

1. Added security: If an end user's wallet is stolen, a thief could use their stolen credit cards quite easily. If the user's smartphone is stolen, if it is passcode-protected, it will be more difficult for the thief to access the user's payment methods.

2. Improves your Merchants' customer service: Merchants and their customers are always looking to cut down on the time it takes to check out at the register. NFC allows your Merchants to provide a faster payment method to their customers that includes improved convenience and ease of use.

3. Versatility: NFC technology can be used in a wide variety of industries and services. It can be used to purchase goods, make both movie and restaurant reservations, and more.

How Does Security Work with NFC Payments?

NFC allows payments to be secure, fast, and convenient. The NFC reader and the smartphone securely pass information back and forth to complete the payment. Here is one example of the process:

1. You use your phone to take a picture of your credit card
2. That data is loaded on the phone
3. The phone provider sends details to your Issuing Bank or network
4. Your bank/network replaces details with randomly generated numbers
5. Security programmed into phone
6. Your payment token is sent back to the phone provider

Other NFC security measures can also include:

Dynamic Encryption – Tokens change every time an NFC transaction occurs, so data is impossible to isolate and extract.

Touch ID – Many phone providers require thumbprints or facial scans to access payments apps.

The Future of NFC

As of 2018, about 25.3 percent of smartphone users in the United States were actively using Near-Field Communication or Contactless Mobile payment Services. Further, according to Statista, in 2023, Near-Field-Communications or other contactless technologies are projected to generate over 220 billion U.S. dollars in transaction value.

Mobile Wallets continue to grow in popularity. In addition to Apple Pay®, Google Pay™, and Samsung Pay®, many retailers are creating their own Mobile Payment methods using Near-Field Communication technology. One example is Starbucks, who now allows customers to use their mobile app to pay at the counter by waving their phone across the payment terminal.

With NFC and contactless Mobile Payments continuing to grow as a preferred payment method, Participants need to be able to offer this technology within their software solutions in order to stay competitive in the ever-evolving payments landscape. Global Payments supports all major digital wallets, NFC and EMV contactless solutions, allowing consumers to pay using contactless cards or the personal devices they carry with them daily.

Section 10: What is EMV Contactless?

The security features built into credit cards have evolved rapidly over recent years. The once ubiquitous "magstripe" (magnetic stripe) gave way to EMV chip cards because EMV chips are more secure than magstripes. A chip card is a payment card containing one or more computer chips or integrated circuits for identification, data storage or special purpose processing used to validate personal identification

numbers (PINs), authorize purchases, verify account balances, and store personal records. Recently, EMV chip cards have further evolved into EMV contactless cards.

Think of EMV contactless (sometimes referred to as "tap-and-go") as the perfect marriage of the security features of EMV technology combined with the ease, speed, and convenience of NFC (Near-Field Communications). NFC is the technology that allows your credit card to communicate with an NFC-enabled terminal at close range. It drives the functionality behind popular Mobile Payment platforms like Apple Pay®, Google Pay™, and Samsung Pay®.

Contactless payments have experienced a significant increase in popularity recently. In 2020, approximately 2.8 billion contactless payment cards were in circulation globally. The growth in issuance of contactless cards accelerated significantly due to the COVID-19 pandemic, which pushed consumers and businesses to adopt contactless payments for hygiene reasons. Contactless cards became especially popular in regions like Europe, where regulations and infrastructure were already in place, and their usage surged worldwide as a safer payment method during the pandemic.

History of EMV Contactless

EMV contactless technology has continued to evolve in recent years. Here is a brief overview of some of those milestones:

1995: UPass – The Seoul Bus Transport Association launches the world's first-ever contactless payment card for commuters, the UPass.

1996: EMV – The first version of the EMV security standard is published in 1996.

2004: Contactless cards used for first time in US

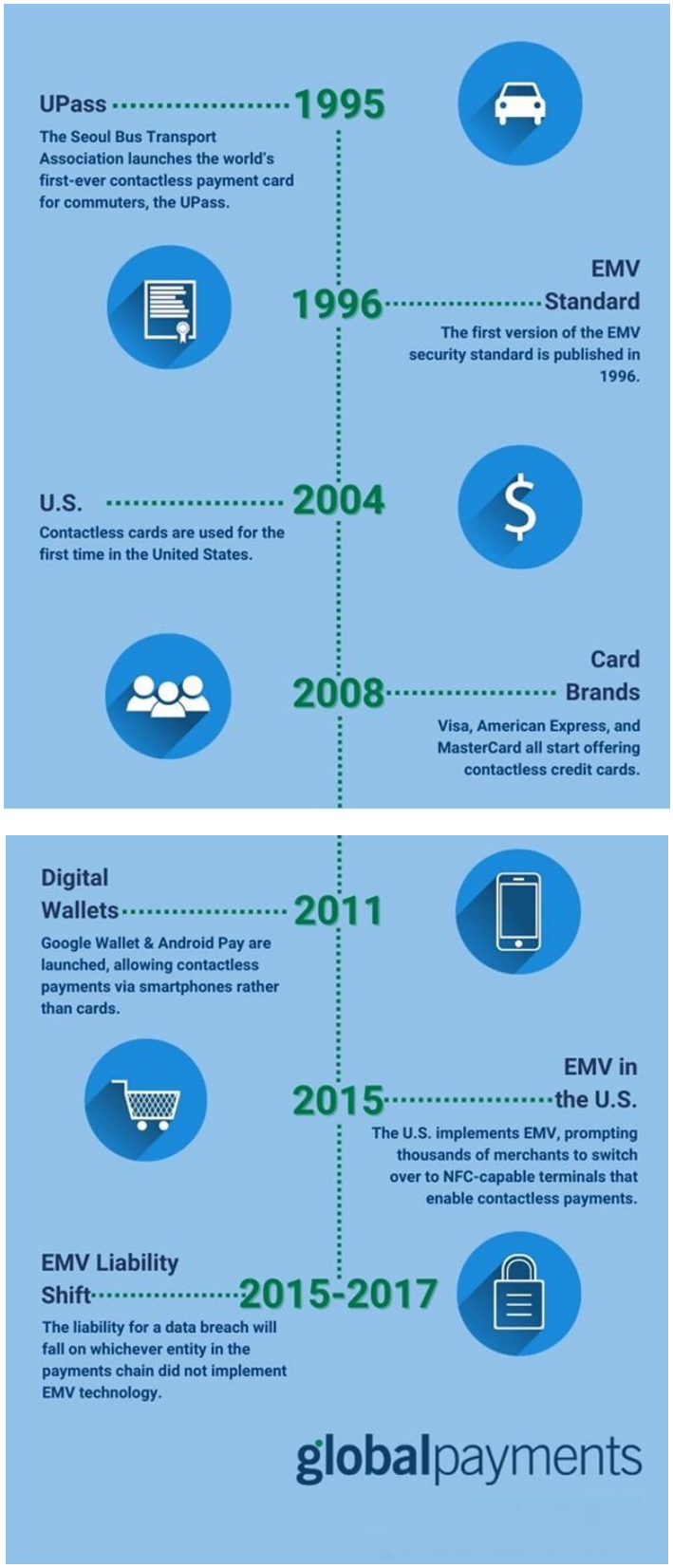
2008: Visa, American Express, and MasterCard all start offering contactless credit cards.

2011: Google Wallet and Android Pay are launched, allowing contactless payments via smartphones rather than cards.

2015: EMV in the U.S – The U.S. implements EMV, prompting thousands of Merchants to switch over to NFC-capable terminals that enable contactless payments.

2015-2017: EMV liability shift implemented – The liability for a data breach will fall on whichever entity in the payments chain did not implement EMV technology.

History of EMV Contactless



Benefits of EMV Contactless

Security *– the chip on a contactless card communicates with the POS device through short-range wireless technology by virtue of an embedded antenna. Upon tapping a contactless card, a cryptographic code is created that is unique to that specific transaction.*

Speed *– The quicker speed of contactless payments is ideal in fast-moving industries who accept credit card payments, such as sporting events, convenience stores and quick-serve restaurants.*

Convenience *– Much of the Participant payment processing experience for Constituents comes down to how quickly they can pay and get out. Credit Card Processors spend untold hours working on ways to help improve the Cardholder checkout experience. Contactless results in a checkout process that could hardly be easier or faster – just tap and go.*

Section 11: Mobile Payment

Within the last five years, Mobile Payments have become increasingly popular and are also being positioned as the new norm in the payments industry. With our money at the tips of our fingers (literally), we are able to pay a friend, family member, or Merchant through smartphones, tablets and other electronic devices. It is estimated in 2020 that over 90 percent of smartphone users will have made at least one Mobile Payment in their life. With this outstanding rate of technologically savvy consumers, it is no wonder Merchants are focusing on more efficient ways to create a seamless experience for their business and clients.

What is considered a Mobile Payment?

If you have paid for a good or service through the use of your smartphone, tablet, or any other electronic device, you have made a Mobile Payment.

Some popular types of Mobile Payments include:

1. Mobile Wallets – Have you gone into Target to purchase goods with the use of Apple Pay®? Or maybe you've gone to your favorite local spot to grab food and pay with your phone. If you have, then you've utilized your mobile wallets to purchase a desired good or service. Popular mobile wallets include Apple Pay®, Samsung Pay®, and Google Pay™.

2. SMS Payments – An efficient way to process a payment is through text to pay. The consumer simply sends an SMS message out to the service provider they would like to pay and in turn they will receive a code to confirm the payment.

3. Point of Sale Payments – Most places of business now have a point of sale (POS) payment device where you can quickly place your phone up to the device reader and it will scan it automatically. This creates a faster and smoother payment process that will help the consumer get the good or service more quickly and in turn helps the Merchant process more payments and create more revenue.

4. Mobile Payment Apps – The Starbucks app, which is currently the most widely used Mobile Payment app, is utilized by going into the store or drive through and then scanning the barcode attached to your app, all while earning points that will lead to future Starbucks perks. Additional apps such as Venmo and PayPal are widely utilized to ease the effort in paying a peer or family member, and only take seconds to send or request the desired amount through the use of the app.

Benefits of Mobile Payments

Convenience – In this digital age, consumers are clinging tighter to their digital devices and less to physical wallets. Consumers no longer have to worry if they forget their wallet as their payment method is stored directly on their smartphone or other digital device. It is very convenient for a consumer to avoid fumbling around for spare change, and instead have the exact amount prepared with a touch of their fingertips and a swipe of a barcode. Using Mobile Payments for parking or at a vending machine are a couple of examples.

Security – Mobile Payments provide an extra layer of security in regard to the traditional credit card. It is tougher for hackers to obtain personal credit card information from mobile wallets and apps since they typically utilize encryption and security codes. In addition, if a physical card is stolen or lost, it is easy to replicate or record the personal credit card information, whereas a smartphone typically has a password or touch ID in order to access secure information.

Rewards – When using mobile apps to make a purchase, such as the Starbucks app, there are typically options for rewards. Most rewards provide incentives, such as purchasing a new item on the menu to earn extra points, and then points are used for a free item or extra percentages off of the next purchase.

According to research conducted by Reuters, in the year 2021, global mobile point-of-sale revenue is expected to reach nearly $50 billion (from just $6.6 billion in 2016). Due to the drastic increase in Mobile Payment usage, it is clear that the new way to pay is mobile. With the convenience and ease of holding your smartphone over the point-of-sale terminal to pay, it is clear to see why consumers are gravitating towards Mobile Payments instead of more traditional ways to make a payment.

Section 12: Contacting ePAY Support

You may contact ePAY's dedicated Help Desk:

Phone: 855.226.7337 (24 hrs. and 7 days a week)

email: ePAYCustomerSupport@illinoistreasurer.gov

ePAY Ticketing Portal: https://epay.jtpyportal.com/Login_Epay.aspx

For current ePAY Participants, please review our training videos for more information about ePAY services and reporting.

Section 13: Glossary of Terms

Glossary of Electronic Payments Industry Terms

ePAY Terms Glossary