NEW 2015 update

WHAT EVERY CARD-NOT-PRESENT MERCHANT SHOULD KNOW

VERIFI™

Navigating Today's Challenging Payments Ecosystem

Preface

Today more than ever, Card Not Present (CNP) merchants face mounting challenges managing a safe and efficient operation. Since this eBook was first published last year a year ago, the payments space evolved, illuminating new opportunities as well as emerging threats and new vulnerabilities. This updated guide follows the path of the card-not-present transaction and provides CNP merchants with a detailed map for navigating the payment-processing ecosystem in 2015 and beyond. We describe the tools, processes and best practices that CNP merchants can use to efficiently and cost-effectively process payments, mitigate pre-sales fraud and risk, manage chargebacks, and improve billing and authorizations. We've also updated the eBook to reflect the new forecast for global payments in the coming years and changes brought about by EMV, mobile payments and other emerging technologies.

This guide will:

- Provide insight into payment processing considerations from start to finish, including security, data protection, compliance and the total cost of authorization.
- Outline steps to mitigate pre-sale fraud, including an overview of current fraud trends and solutions.
- Discuss total chargeback management – how to prevent chargebacks and also recover revenue lost to chargebacks.
- Explore the impact of card declines on profitability and customer retention and learn how to improve authorization success.
- Examine how merchants that properly understand regulatory requirements and industry best practices for fraud prevention, risk management and authorization optimization will be better equipped to navigate the complex CNP payments landscape.

Merchants that properly understand regulatory requirements and industry best practices for fraud prevention, risk management and authorization optimization will be better equipped to navigate the complex CNP payments landscape.

Table of Contents

Effective Payment Processing

Getting Set-up for Success

Chapter 1

This chapter discusses ways to help merchants navigate numerous payment processing decisions and better understand the cost of compliance, security and the total cost of acceptance.

From building and maintaining a secure, cost-effective payment process to better understanding PCI compliance, this section provides insight into the CNP payment ecosystem including:

- Rates and Fees
- Pros and Cons of Processing Types
- Secure Payment Processing
- Compliance vs. Non-compliance
- Total Cost of Acceptance

Understanding the Basics

The first step in setting up your payment processing is to establish the proper type of merchant account. There are many types of merchant accounts and each offers different rate and qualification requirements depending on your business type and transaction volume.

- The Merchant Category Code (MCC) is a four-digit number assigned to your business by the credit card company and classifies each business by the type of goods and/or services provided.[1] It's important that your MCC is properly defined as it plays a key role in determining approval rates and rate qualifications as well as the interchange fees your business pays. Some MCCs may qualify a business for rates specific to their industry.

Your gateway provider should be your partner. When selecting a payment gateway, merchants should pay attention to costs: there are absolute costs like rates and fees that are simply a part of doing business but there are a number of options that can be configured to a merchant's business needs and goals:

- Merchants should consider the different costs associated with each card brand; some may cost more to process than others. Meeting all qualification requirements can decrease the costs incurred by processing more expensive card types.[2] Watch out for overlooked items like contract termination and hidden fees.

- Integrated payment solutions help reduce manual errors and reduce cost.[3] By merging payment processing with business solutions, merchants can automate payment reconciliation with accounting and other business processes, cutting down on redundant data entry and eliminating the potential of human error.[4]

Choose a provider that is flexible and able to adapt as your business evolves. Whatever the size of your business, work with your provider to achieve the right balance of rates and fees.

Rates and Fees

Rates and fees are a fact of life. Merchants pay transaction processing fees, which are dependent on both personal and business risk, average dollar amount per sale, total dollar amount of monthly sales and percentage of CNP sales.

Rates and fees are numerous and complex. Here are some primary ones to consider:

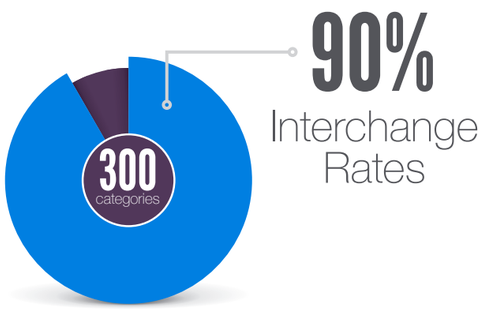
RATE TYPE	TYPICAL CLASSIFICATION
Qualified rate	This rate is typically the lowest rate a merchant can receive and is charged for processing regular credit cards by an approved processing solution.
Mid-qualified rate	This rate is the next lowest tier of rate a merchant can receive and is typically charged for manually keyed-in card transactions as opposed to swiped transaction. This rate is also typically charged for rewards and/or business cards.
Non-qualified rate	This rate is charged for transactions involving cards that do not qualify for the qualified or mid-qualified rates. This may include transactions where there is no address verification, a card is manually keyed-in, the authorization does not settle within the allowed time frame or if other information is missing. A merchant's rate may increase (down grade) when transactions do not qualify for the lower rates.
Interchange fee	This fee covers credit losses, fraud and authorization costs and is calculated as a percentage of the transaction. This fee may also be included in the bundled rate offered by merchant service providers. Merchants may request that they pay interchange fees on occurrence rather than as part of a bundled rate to better track transaction costs.
Chargeback fee	This fee occurs when a cardholder disputes a transaction, which is then returned to the acquiring bank. Fees vary by provider and may increase with delayed responses from merchants to a chargeback inquiry.[5]

Interchange Rate Considerations

Interchange rates are fees that the acquirer pays to the Issuer and passes through to the merchant. Interchange rates are set by the payment networks like Visa®, MasterCard®, and Discover®. There are many factors that impact the interchange rate:

- CNP transactions are typically subject to higher interchange rates than card-present transactions.
- Premium credit cards generally have a higher interchange rate than standard credit cards.
- Standard credit cards tend to have a higher rate than signature debit cards, which in turn have a higher rate than PIN debit transactions.[6]

Interchange rates may occur as a pass-through charge or as part of a bundled rate. Depending on the factors at play in your business and for any specific transaction, you can pay the best rate or face higher rates when transactions are downgraded – generally the payment networks quote a low rate for a transaction based on meeting a number of requirements (card type, type of business, etc.) If you don't meet the requirements of the transaction, you are downgraded to a more expensive interchange rate.



DID YOU KNOW?

INTERCHANGE RATES make up nearly 90% of the direct cost of every transaction. In all, there are more than 300 interchange categories impacting rates.[7]

The Who's Who of Payments

Payment Facilitators (PayFacs)

PayFacs facilitate payments on behalf of merchants (called sub-merchants) by contracting with them for a suite of payment services that includes processing and funding. By aggregating the transactions of sub-merchants (tracked and reported with sub-merchant ID fields and soft descriptors), PayFacs help merchants who lack a traditional acquiring relationship increase card acceptance, adding value to the payment ecosystem.[8]

Payment Service Providers (PSPs)

PSPs are typically SaaS companies that offer a single payment gateway for merchants to accept electronic payments through multiple payment methods, including credit card, bank transfer, direct debit and real-time bank transfer. As a payments hub, these PSPs connect to multiple payment networks, acquiring banks and card brands and often fully manage these connections and relationships, freeing up the merchant from dependence on financial institutions and the burden of establishing direct connections with these entities. Since PSPs often work in bulk, they offer merchants cheaper fees than the cost of working directly. Full-service PSPs may also offer fraud and risk management services for CNP payments, analytics and reporting and other services along the payment spectrum (multi-currency, next gen payment systems, paper & e-check processing). The industry sometimes refers to PSPs as payment gateways, though the services they can provide are typically much broader.[9]

Internet Payment Service Provider (IPSPs)

IPSPs offer an all-in-one CNP payment processing solution for e-commerce merchants. They aggregate third-party processing solutions through a sponsored or shared credit card processing account, giving merchants access to all the services and technology necessary to manage and protect payments from end to end.[10] IPSPs simplify CNP commerce for all merchants, but particularly those with limited IT or other resources. Through shared risk and alignment of business priorities between IPSPs and merchants, merchants can shift their focus to business goals, leaving the complex details of secure, efficient payment processing to their IPSP partners.[11]

New Methods of Pay & Implications to the Ecosystem

New payment methods are emerging daily and consumers may soon be cashing in their wallets for alternative types of payment, including mobile wallets, peer-to-peer (P2P) payments and social payments. As the increased need for a secure way to pay meets consumer desire for more convenience, technology companies have developed payment methods to satisfy both. We've outlined some of the more popular methods below.

TYPE	EXAMPLE	WHAT IT IS	IMPACT ON PAYMENTS
Mobile Wallets	Apple Pay, Google Wallets	The use of NFC technology to make proximity payments via smartphones at POS terminals.	New technology like Near-Field Communication (NFC) has opened up new sales opportunities for merchants who can harness that data in a meaningful way. This push toward loyalty will force it to evolve from its current state as hard to track and measure and expensive.
Peer-to-Peer (P2P) Payments	Chase Quick Pay, PayPal	The ability for users to send money directly to another person from their mobile device using existing payment infrastructures like card networks, ACH or intra-account transfers.[12]	P2P payments offer convenience for intra-personal payment in many cases; however, when security measures become too burdensome or there are too many hoops to jump through, users may abandon this type of payment method. It's also important to note that in the case where payments are made originating from a checking or savings account, or a credit card, the transaction/transfer is protected under federal law.[13]
Social Media Payments	Facebook Messenger Payments	Service allows users to connect their credit card information to Facebook and make P2P payments online through an encrypted connection facilitated by Facebook's service.[14]	The service rolled out by Facebook does not charge fees because it doesn't need to monetize payments.[15] As one of the largest apps in the world, Facebook Messenger Payments prevents users from having to leave the app to go to another service to make payments, keeping users engaged without interruption.[16] The convenience afforded by this technology could skyrocket the use of P2P and micro-payments as commonplace.[17]

Understanding the Pros and Cons

Merchants should understand the pros and cons of various gateway features and processing considerations.

CONSIDERATION	PROS	CONS
Real Time Payment Processing	Allows CNP merchants to keep up with the need for real-time account updates and expedited payment processing. Can be used as a means to avoid disruption of service (e.g. cell phone services, utilities, etc.). Reduction in data processing errors, which can be fixed instantaneously and help give merchants more control over inventory and inventory turnover. Increased customer satisfaction by avoiding delayed billing and reducing the use of paper.[18]	The auditing of a real-time processing system can be costly and time consuming and requires a backup to maintain the integrity of the data. For some merchants, real-time processing may add more risk to the payments process than perceived benefit.[19]
Batch Processing	The ease-of-use for batch payment processing allows merchants to initiate the data process without requiring constant supervision, allowing for faster payments and streamlined reporting. The automation of batch processing reduces the need for manpower and increases efficiency by requiring less computer processing time and creating a solid audit trail.[20]	Batch processing can be slow and there may be a time delay before transactions are processed and returned. Requires maintaining a current master file.[21]
ADDITIONAL FUNCTIONALITY AND SUPPORT OF ALTERNATIVE PAYMENT METHODS		
Automated Clearing House (ACH) Payment Processing	ACH payments are immediately credited to accounts, reducing the occurrence of manual errors that can happen with paper checks, and automating the collection of bad checks through the ACH processing service.[22]	There are costs associated with ACH processing, including transaction fees and setup costs. ACH differs from a wire transfer in that the money may not be available for immediate withdrawal. Additionally, lack of funds or disputed charges may cause a customer's bank to withhold the money, preventing payment to the merchant.
E-Check Payment Processing	Reduces processing costs in comparison to paper check processing or credit card transactions, saving up to 60% in processing fees.[23] Merchants typically receive funds sooner than they would via paper checks; funds can be received within one business day. Allows merchants to accept out-of-state and international checks virtually risk-free as this type of payment requires customer authentication processes and account validation to prevent fraud and identify bad checks in real-time.	Money paid by eCheck is immediately debited from the consumer's account as opposed to paper checks, which often take several days to process. The potential exists for higher insufficient funds which can delay provisioning of products or services and lead to some customer dissatisfaction.
Cross-Currency	Cross-currency allows merchants to settle in one currency for transactions submitted in multiple currencies, resulting in a consolidated payment to a single bank account.	There may be location-specific exchange restrictions when using cross-currency solutions.
Multi-Currency	Multi-currency options can boost sales and customer experience. The key lies in identifying locations where this added feature makes sense.	Some locations where card brands like MasterCard and Visa account for the majority of CNP sales do not require local payment options, whereas other places may rely on local or alternative options to purchase goods.[24]

Ability to support additional forms of payment, like:

Best Practices for Secure CNP Payment Processing

MasterCard SecureCode SecureCode enhances security by requiring cardholders to enter a private code when making an online purchase with participating retailers, preventing unauthorized use of credit cards.

CVV2 Verification By requesting the three-digit code as part of the CNP process, merchants can be sure that the person placing the order has the card in his or her possession, adding another layer of security.

AVS Authentication Utilizing AVS allows merchants to verify the cardholder's billing address with the data on file with the issuing bank.

Verified by Visa® This service provides verification and validation of a cardholder's ownership of an account in real time by prompting customers to enter a password used to confirm the cardholder's identity by the Issuer.

The best way to understand your real gateway requirements is through reporting and analytics. When selecting a payment gateway and considering the various payment processing types, make sure to demand robust reporting and data analytics features. Reporting provides line-of-sight into recent changes to business priorities and helps you develop custom strategies to address the shifting economics of the business or to prepare for upcoming events. There are a number of reporting metrics and analytical functions you should consider when choosing a gateway:

- **Authorization performance analysis** Predictive modeling can provide insight into the long-term value of customers and aid in the improvement of profitability ratios.
- **Risk assessment analysis** Completion of an overall evaluation of fraud, chargeback, refund, and decline risk assessment assists in understanding the high-risk components of the business.
- **Custom analysis** Every business is different, so CNP merchants should consider relevant analyses and reports they may want to custom build based on their industry and business operations.
- **Overall profitability analysis** Evaluation of all transaction volume leads to the creation of a logical segmentation of the entire business which are then ranked by profitability; solutions may be crafted to address low or unprofitable segments while marketing dollars can be more effectively spent on highly profitable channels.
- **Chargeback, fraud & refund forecasting** Predictive forecasting of chargeback, fraud and refund activity allows for appropriate preparations and adjustments to minimize risks associated with processing for the business.

Safe and Secure Payment Processing

Compliant payment processing protects merchants from costly breaches but also boosts customer confidence and minimizes reputational damage. But merchants that are compliant are still at risk of data breach. That is why maintaining additional layers of security across the entire payment life cycle is essential. While PCI compliance is mandated, security-optimized transaction processing is not. CNP merchants should be prudent in insulating their payment processing operation beyond the requirements of PCI with adequate **data protection, tokenization** and **end-to-end encryption**. Secure transaction processing requires vendor-specific payment protocols that reach from the point of origin, through the network, to the originating point upon receipt of authorization.

DATA PROTECTION

PCI compliance is only one step in protecting data. CNP merchants should be sure that they and their chosen payment processor are PCI certified and take additional steps to guard against data and security problems.

- **Encryption** CNP merchants should encrypt data being sent across public networks, including phone lines, FTP and email.
- **Merchant partner data protection** Merchants are responsible (and liable) for cardholder data accessed by business partners and should ensure that any marketing affiliates, fulfillment houses or other vendors are adequately protecting cardholder data.
- **Limited access to cardholder data** Business processes and operations will sometimes require that other departments have access to cardholder data; CNP merchants should restrict access to sensitive data to only those departments that need it and should enlist the help of their payment processor to set up role-based data access.
- **Secure data storage** Online merchants should never store customer card data on their servers or on a system outside of the firewall. Additionally, information stored internally should be encrypted or not stored at all and tokenized.
- **Transaction routing analytics** When using multiple processors, analytics provide the visibility and monitoring necessary to avoid traffic problems and proactively uncover network vulnerabilities that can often be hidden under layers of routing redundancy.

DID YOU KNOW?

Worldwide, the average total cost of a data breach has increased a whopping 15% in the past year, totaling $3.5 million, with the least expensive breach costing the company $750,000 and the most expensive breach costing almost $31 million.[25]

TOKENIZATION

Part of end-to-end secure transaction processing is tokenization. Tokenization replaces sensitive user data with a reversible benign substitute.[26] As an augmentation to PCI compliance, tokenization simplifies validation by reducing the number of components for which PCI requirements apply, though this solution does not eliminate the need to maintain PCI compliance.[27] There are different implementations of tokenization, from de-tokenization methods to deployment models and technologies. The importance lies in protecting the process and maintaining strong security controls to ensure the effectiveness of the tokenization process and continued compliance.

The main benefit of tokenization is the protection offered to consumers, as their information is guarded from being released to hackers. Additionally, tokenization offers merchants coverage against potential damage not only to their business, but also to their reputation. As evidenced by the recent Target hack, when retailers fail to protect themselves against a major security breach, they become liable to each and every person whose information has been compromised.

Tokenization does have some drawbacks. It is an all or nothing approach to security, and cannot be implemented in pieces, unlike other solutions. With tokenization, several other aspects of security have to be in place to guarantee a safe environment for data. It is not a magic wand ensuring security; it works in conjunction with a comprehensive security policy.

EMVCo TOKENIZATION STANDARD

As the EMV liability shift approaches, the card brands (Visa, MasterCard, Amex® and more) have been working on a global standard for developing tokenization technology.[28] Managed by EMVCo, the standard will take the security of a physical EMV chip and attempt to replicate it in the CNP environment, including online, mobile and proximity payments by tokenizing cardholders' card numbers and including a dynamic component with each transaction to mask the valuable information.[29] This attempt at reducing digital fraud provides merchants with more secure transactions, reduces chargeback risk, improves speed to checkout, enhances payment acceptance options and opens the door to new selling avenues. Consumers benefit from better, easier, faster and more secure ways to pay through a variety of devices, all with an improved user experience at checkout.[30]

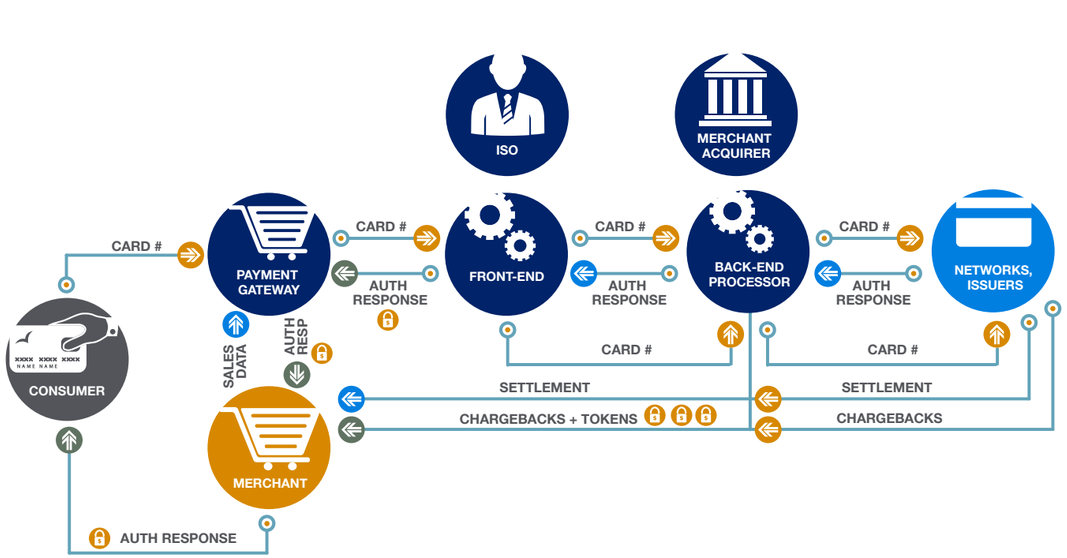
Version 1.0 of the EMV Payment Tokenization Specification was published in March of last year and emphasizes the need for a consistent approach for token routing and authentication as well as data message formats to promote the interoperability of tokens. The framework promotes limiting payment tokens for use in a specific environment but also provides guidance in advancing existing ecosystems to become globally interoperable.[31] In this way, the new standard is compatible with the current payment infrastructure as well as EMV chip specifications, promising consistency across all payment ecosystems.

This global alignment initiative is an answer to the obvious need for consistency in identifying and verifying payment token requests and managing how, where and when a payment token can be used. A consistent approach to data fields and how transactions gateway through the payment ecosystem will aid in eliminating data vulnerabilities throughout the transaction process.[32]

END-TO-END (E2E) ENCRYPTION

End-to-end (E2E) encryption works hand-in-hand with tokenization to ensure complete security of cardholder data, from point-of-sale throughout the entire transaction lifecycle.[33] By encrypting the data at the e-commerce payment software and maintaining encryption throughout, the card number is never stored unencrypted by the merchant.

Typically, merchants store customer cardholder data before it moves into the payment process, putting it at risk if a breach were to occur. With E2E encryption, the card number is separated from sales information and replaced with a token, and the transaction is processed independent from the merchant via controls in the front-end and back-end processes. This protects sensitive information from would-be thieves, who cannot commit fraud with the meaningless token information.



Choosing a Payment Processing Partner

In addition to gateway features and processing options, merchants should consider the end results they need and want in a processing partner. Given the current landscape and constant changes to the marketplace, merchants need a gateway that is equipped to manage today's challenges and is agile enough to adapt to emerging technologies and demands of tomorrow. From safe, secure transaction processing and fraud and risk mitigation to improving authorization and omni-channel optimization, there are a number of capabilities merchants need to evaluate when considering a processing partner. Some considerations include:

- **Global view of business priorities** To optimize profitability, merchants need a global view of business priorities and robust reporting capabilities. Big data and advanced analytics technology is essential to provide mobile wallet and loyalty users with a personalized shopping experience. One-to-one customer engagement and the ability to assess consumer shopping behaviors across channels and provide personalized offers based on the data will separate successful merchants from the rest of the herd. Merchants need to cater to the consumer expectation that offers be personalized and relevant.[34]

- **Safe, secure purchasing experience** Since so much data is involved, security must be a top priority. Mobile wallet providers, in particular, face consumer skepticism over the collection and use of personal data. Merchants cannot afford to work with a processor that is unclear about their transaction security. Fifty-seven percent of mobile app users in the U.S. have declined to install an app or have uninstalled an app over concerns about how personal data is used.[35] The rise of omni-channel commerce has opened up new sales opportunities, but also significant new vulnerabilities.

- **Chargeback fraud and risk mitigation** Between EMV, NFC, mobile and other emerging technologies, fraud is escalating across channels and becoming more complex. As new vulnerabilities are being discovered daily, chargeback prevention and recovery and fraud and risk management are essential components of any gateway. Data security and rising fraud statistics illustrate the devastating effects non-secure processing has on a merchant's brand and bottom line: roughly 60% of fraud victims reported a significant decrease in trust of retailers after having their data compromised.[36] Merchants can't afford the brand damage that comes from non-compliance, inadequate security measures or data breaches.

- **A way to lower attrition and churn** You cannot improve customer loyalty if you are bleeding customers and the cardinal sin of commerce is to lose customers that WANT to continue paying you. The first step for merchants is providing a seamless, personalized customer shopping experience that entices consumers to shop. Merchants must also ensure that they aren't losing customers to unnecessary card declines. The cost to acquire a new customer is 4 to 10 times more expensive than retaining an existing one[37], so involuntary churn has a significant impact on merchants' long-term revenue streams.

- **Adapting to emerging technology** The rise of omni-channel commerce has opened up new sales opportunities, but also significant new vulnerabilities. Lack of real-time insight and the cost of updating legacy systems that don't offer comprehensive reporting can inhibit your profitability. Processors should be scalable and flexible to support change and business growth. Inflexible or limited processing options can cause decreased performance, increased costs and processing bottlenecks that degrade the customer experience and hurt sales. Merchants must be able to affect positive changes and scale, grow and adapt to the changing payments landscape. A static solution will not be enough.

Merchants should choose a partner with a thorough understanding of the challenges of the current marketplace and that can offer agility and seamless integration to adapt to emerging needs and threats. Ideally, a gateway partner will provide end-to-end chargeback, fraud and security protection, deep insights from real-time analytics and reporting and a way to salvage unnecessary card declines.

Increased Regulation and Oversight Impacts Merchants & Issuers

EMV is just the tip of the iceberg when it comes to the pressures of global standards, increased regulation and stricter oversight. Increased regulations on banking and payments and additional focus on consumer protection are forcing merchants and Issuers to become more vigilant in protecting payments. Industry regulations have historically sided with consumers, giving them increased ability to actively dispute payments with almost no consequence. Issuers, on the other hand, must comply with new oversight through processes outlined by several agencies like the Consumer Financial Protection Bureau (CFPB) and the Payment Network Association (PNA). These pressures include PNA guidelines that frequently change, complex documentation and the need to meet Regulation Z (Truth in Lending Act). As the volume of chargebacks continues to grow, accommodating these dynamic standards and regulations becomes burdensome and costly for Issuers.

To relieve that burden and in the interest of customer retention, many Issuers are prone to issue temporary credits to cardholder accounts in response to disputes. This frees the consumer from the responsibility of paying for the good or service; however, that process adds cost and risk to the entire payment ecosystem. When cardholders bypass the merchant and go directly to the Issuing bank to dispute a charge, merchants pay a hefty price in fines, fees, penalties and the cost of goods or services lost. In short, the entire payment ecosystem suffers.

Compliance in Payment Processing

Merchants need to ensure their business is compliant with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is "a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information."[38] This standard was created by Visa to provide merchants with consistent data security protocol.

PCI DSS compliance can have great benefits for merchants, including increased customer confidence that the merchant is adequately protecting sensitive card information. The PCI DSS is comprised of twelve security requirements - each consisting of numerous tasks and steps to complete - to protect cardholder data. We've updated this section with information about PCI DSS 3.1 as a result of the Council's continued development of the standard within the framework of a defined 36-month lifecycle consisting of 8 stages.[39] In addition to the changes to PCI DSS, merchants should be aware of the impact EMV migration will have on their business from a regulatory standpoint as well as the added costs incurred as a result of supporting the new technology.

GOALS	PCI DSS REQUIREMENTS – VALIDATED BY SELF OR OUTSIDE ASSESSMENT
Build and maintain a secure network	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
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	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
Regularly monitor and test networks	10. Track and monitor all access to cardholder data
	11. Regularly test security
Maintain an information security policy	12. Maintain a policy that addresses information security

Find the Right Balance

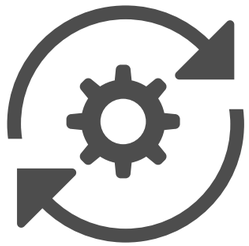
Compliance is not a one-time occurrence: it is ongoing. For that reason, there are four levels of compliance and associated costs for CNP merchants to consider.[40] The cost of compliance includes the infrastructure and technology costs associated with closing the gaps identified in the merchant's current business model. Annual costs refer to the costs to maintain PCI compliance from year to year.

LEVEL	MERCHANT CRITERIA	COMPLIANCE REQUIREMENT	ANNUAL COST
Level 1	**Visa, MasterCard & Discover** Any merchant that processes greater than 6 million credit card transactions per year via any acceptance channel.[41] **American Express** 2.5 million or more American Express Card transactions per year.[42]	Annual PCI data security assessment conducted onsite by a third party vendor in addition to quarterly network scans.[43]	**Initial scope** - $250,000 **Becoming compliant**- $550,000 - $1,000,000 Annual PCI cost - $250,000
Level 2	**Visa, MasterCard & Discover** Any merchant that processes 1 to 6 million transactions regardless of channel.[41] **American Express** 50,000 to 2.5 million American Express Card transactions per year.[42]	Self-assessment conducted annually by a third party vendor in addition to quarterly network scans.[43]	**Initial scope** - $125,000 **Becoming compliant**- $260,000 - $500,000 Annual PCI Cost - $100,000
Level 3	**Visa, MasterCard & Discover** Any merchant who processes 20,000 to 1 million online transactions per year, regardless of channel.[41] **American Express** Less than 50,000 American Express Card transactions per year. [42]	Self-assessment conducted annually by a third party vendor in addition to quarterly network scans.[43]	**Initial scope** - $50,000 **Becoming compliant** - $75,000 - $90,000 Annual PCI cost - $35,000
Level 4	**Visa, MasterCard & Discover** Less than 20,000 e-commerce transactions or 1 million total transactions via any channel.[41]	Self-assessment conducted annually by a third party vendor in addition to annual network scans.[43]	**Initial scope** - $50,000 **Becoming compliant**- $75,000 - $90,000 Annual PCI cost - $35,000

PCI 3.1

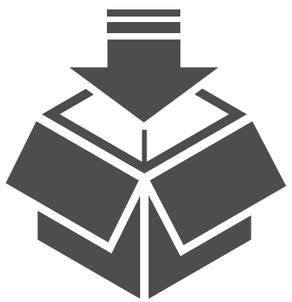
Credit card security has been caught in an endless loop for years: hackers continue to use more sophisticated technology and solution providers continue to provide more high-tech ways for merchants to defend against hackers. The PCI Council released its standards for 3.1 in the hopes of helping companies limit the scope of PCI DSS.

Major Updates



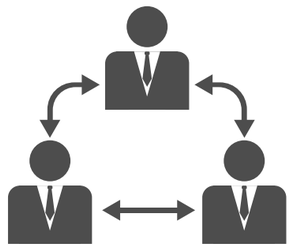
#1 Penetration Testing

Merchants must verify the methods they use to segment cardholder data environments (CDE) from other areas, and both internal and external penetration testing activities must follow an "industry-accepted penetration testing methodology."[44] Smaller merchants who leverage the help of an outside vendor will need to ensure that the penetration testing solution they choose adheres to one of these industry-accepted methodologies.



#2 Inventorying System Components

This new requirement means merchants must compile a list (if not already existing) of hardware and software components – including descriptions of both the function and use for each – involved in the CDE.[45]



#3 Vendor Relationships

This requirement specifies that all vendor relationships as they relate to the management of PCI DSS requirements be explicitly outlined. This includes the explicit documentation of segregation of roles wherein the merchant manages a part of a duty and the vendor manages another portion (in the case of a hosted data center, the vendor may manage the physical access restrictions of the data center whereas the merchant manages providing access to those locations).[46]

#4 Antimalware

Merchants must "identify and evaluate evolving malware threats" for "systems considered to be not commonly affected by malicious software." For merchants utilizing systems not typically affected by malware such as Unix servers, a process must be created to ensure that these systems continue to remain unaffected by malware OR that the merchant will remain aware of any new malware that emerges specific to those platforms. Additionally, it's now mandated that the disabling or altering of antivirus mechanisms be authorized by management in a time-limited fashion. The antimalware system must also be able to lock out a user from disabling it.[47]

#5 Physical Access and Point of Sale

Merchants are required to control the physical access of on-site personnel, with the ability to authorize the level of access per individual job function and immediately revoke access in the case of termination. Merchants must also "protect devices that capture payment card data…from tampering and substitution."[48]

The Bottom Line

The bottom line is that non-compliance is much more expensive than compliance. Fines for non-compliance can range from $5,000 to $100,000 per month at the discretion of the payment brand. This cost is typically passed through the bank and eventually rests on the merchant. Another risk is termination of relationships with your merchant bank in addition to raised transaction fees.[49]

If a data security breach takes place, a fine of $50-$90 per cardholder compromised can be imposed, along with an increased risk of civil suit brought by customers.[50] Credit card account providers can also penalize merchants by suspending acceptance. Aside from the dollar amount, brand and reputational damage risk can be costly as well.

DID YOU KNOW?

According to a 2011 study, the extrapolated average cost of compliance for organizations exceeded $3.5 million, with one Level 1 company paying over $16 million.[51]

The Future Impacts of EMV on CNP Commerce

As EMV rolls out in the U.S., CNP fraud is predicted to more than double by 2018, from $2.8 billion to over $6.3 billion. EMV chip technology has been deployed in other countries for years and is quickly becoming the global standard for helping secure physical credit and debit card and Visa to develop a smart chip technology that embeds microprocessor chips that securely stores cardholder data on payment tools (payment cards, mobile phones and others). In the U.S., this technology is known as “chip cards.[52]

For Visa merchants, liability will shift to acquirers if the merchant lacks an EMV-enabled POS device for both domestic and cross-border counterfeit fraud card-present POS transactions.[53] In short, non-compliant acquirers and merchants will assume liability for all fraudulent transactions at that point – a costly assumption considering that liability is estimated at more than $10 billion in the U.S this year alone.[54]

One of the biggest vulnerabilities in CNP commerce is authentication. The method of authenticating users by user-name and password doesn’t work as is evident with the recent data breaches. 3D Secure is a valuable tool that provides liability protection for merchants by reducing the likelihood of fraud in those transactions that implement it. It also gives merchants and Issuers more control over card fraud and chargebacks by authenticating cardholder identities and assessing transaction risk while creating very little friction in the customer purchase process. This hasn’t always been the case, but with enhancements like dynamic authentication and the reduced use of pop-up windows, 3D Secure has become more user-friendly.[55]

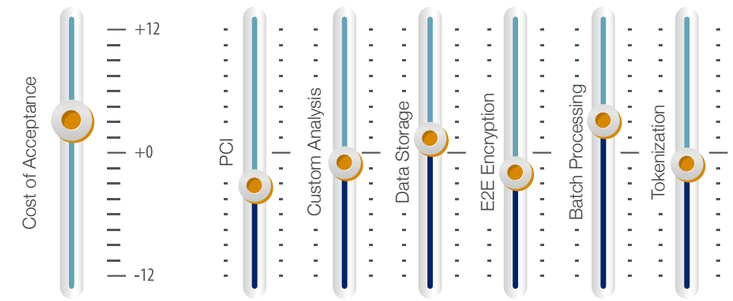
The best fraud prevention strategy will allow you to manage data points and back-end feedback loops. Proactive use of this information and the ability to adjust quickly will be key to protecting your business. Unfortunately, often times this will be complicated as a result of having to juggle multiple vendors or integrations.

Merchants Need to Weigh the Total Cost of Acceptance

The total cost of acceptance will vary from merchant to merchant and is dependent on a number of considerations. CNP merchants must weigh cost, benefits and limitations of payment processing options.

By following industry standards and best practices along every step of the payment process, businesses have the opportunity to decrease many of these costs and even increase revenue. Payments-related expenses are a cost of doing business, but – when managed properly – can be a driver of increased efficiency, growth and long-term stability and savings.

Merchants must take into account a number of considerations to achieve a balanced payment processing system for their business.



Protecting Your Sales Process from Fraud:

Fraud Trends & Tools

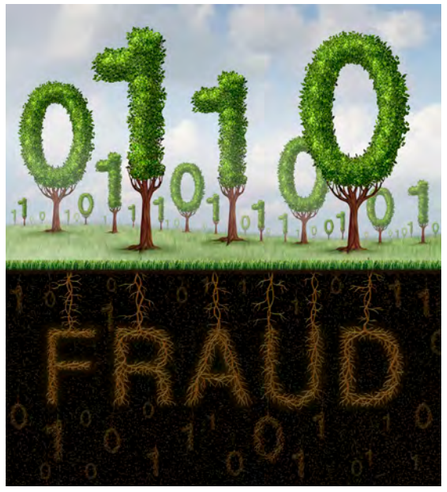
Chapter 2

This chapter looks at some of the recent trends and root causes of fraud, reviews some of the current and emerging fraud prevention technologies as well as comprehensive risk management strategies that can be pursued.

Fraud: A Growing Problem

A number of market forces including mobile payments and data vulnerabilities caused fraud to skyrocket in 2014. Annual fraud costs soared 38% over 2013, reaching $32 billion last year.[56] We saw the impact of mega retail data breaches in 2014, raising the cost of fraud significantly: merchants pay $3.08 for every dollar lost to fraud – up from $2.79 in 2013.[57]

EMV will only aggravate the problem for CNP merchants and Aite Group predicts that online fraud will more than double to $6.3 billion by 2018. In largely eliminating card-present fraud, the global standard will shift criminals to the cyber realm where the chip & PIN security features are irrelevant.



DID YOU KNOW? **Mobile fraud cost merchants dearly in 2014 – every $100 of mobile fraud cost $334, up $51 over 2013.[58]**

EMV Will Impact CNP Fraud

EMV will force fraudsters to the online channel and e-commerce merchants need to be prepared. Given the recent data breaches and overall increases in e-commerce fraud, account takeover and card fraud are top of mind for merchants. The rollout of EMV is widely expected to increase these risks as the CNP channel becomes the most accessible and profitable route for fraudsters.

Merchants must start now to increase security against the more sophisticated types of attacks that will emerge. Current tools will likely no longer be enough to secure a merchant's business customers against fraudsters. The Aite Group says that nearly 75% of all retailers have no idea that a new "chip and pin" system is about to be introduced, leaving more tools for the business to deploy in your pre sale and post sale process to address these increased risks without turning away perfectly good sales.

Common Types of CNP Fraud

CNP fraud is constantly evolving and new threats emerge daily. 2013 and 2014 brought the real danger of data breaches to light. Friendly fraud accounts for $11.8 million in losses annually. There were 75 million new strains of malware identified in 2014.[59] From hacking and friendly fraud to social engineering and malware, fraud is here to stay. Fraudsters are clever. It seems like every day security companies are documenting fraudster's new and innovative methods for separating CNP merchants from their hard-earned money. The migration to EMV will largely eliminate most card-present fraud; however, that fraud will be displaced to the CNP channel. Additionally, the benefits of EMV on card-present transactions will be slower to come to fruition than initially predicted as only 20% of merchants are forecasted to have compatible POS systems by the end of 2015.[60]

Phishing Phishing is a serious and increasing problem that occurs when fraudsters try to obtain sensitive information (usually usernames and passwords or credit card or bank account numbers) in an attempt to utilize this confidential data to make fraudulent purchases or steal a person's identity. The attempt to steal information is made via electronic communication like an email or instant message and leads victims to a website asking to submit this sensitive data.

Account takeover Account takeover is another serious type of fraud that compromises a user account and puts sensitive information at risk. Fraudsters target web users while the users are accessing their various accounts, email addresses and social networks with the goal of stealing these credentials to make fraudulent purchases. With the rampant occurrences of data breaches in 2014, this has become a popular method for cybercriminals. The use of Remote

Access Trojans (RATs) help fraudsters circumvent device ID and second factor authentication to control a system as if they had physical access.[61] Data thieves can then absorb the identities of unknowing cardholders, using their acquired payment card data to make fraudulent purchases both online and in-store (with counterfeited cards).

Carding Carding happens when fraudsters use websites with real-time transaction processing to validate stolen card information (credit card numbers and personal data) by making a small purchase so as to not attract attention to their activity. If their fraudulent purchase goes through, signaling that the card is good, fraudsters will use the stolen card number to make additional purchases or will sell the information to other criminals.

Malware 2014 was a record year for cyber attacks and set the record in terms of malware create levels – more 200,000 strains were detected daily.[62] Potential attackers can either use phishing to mislead the victim to install a malicious app or exploit another remote vulnerability of some app and conduct background monitoring. A malicious app can disguise itself as an app that runs in the background (e.g. music) to conduct monitoring, disrupt computer operation, gather sensitive information, or gain access to private computer systems. Many types of malware aim to collect a record of a user's activity to gain access to sensitive credentials or login information, which can then be used to make fraudulent purchases if payment card data is found. New strains of malware go to heroic measures to avoid detection and analysis, with some rendering the machines they infect unusable.[63]

Location masking This threat does not directly affect cardholders but occurs when a fraudster masks their true location and computer characteristics. The fraudster's machine typically masks many of its features. For example, the browser being used may be Firefox but may be reported as IE9, the operating system may be Linux but may be reported as Windows, and the IP address may be misrepresented, hiding the true location of the fraudster. Online services, websites and applications typically rely heavily on IP location information to function – e.g. a business may provide general information over the web, but completely deny online service requests from locations where it does not have a presence.

THE CRIMINAL MIND

SOME POPULAR SCHEMES ON THE RISE

Threat 1 **Hackers gain access to POS systems via stolen credentials**, giving them access to sensitive payment card data when merchants do not properly segregate their POS systems the rest of their network.

Threat 2 **Anonymizing proxies** allow fraudsters to use stole or fraudulently obtained credit card data to make purchases or commit click fraud.

Threat 3 Criminals have learned to thwart cookies and other inconsistent identifiers when making fraudulent purchases online, making it more difficult for merchants that **implement digital fingerprinting or other technologies to detect.**

Threat 4 Criminals leverage **affiliate networks** to commit fraud through seemingly legitimate marketing channels, making it very difficult to detect.

Threat 5 Merchants are falling prey to increasing cases of **friendly fraud** where chargebacks are used as a form of shoplifting and customers claim they never received goods or services because of buyer's remorse.

Fraud Solutions

The challenges posed by EMV mean that merchants need to focus on their biggest vulnerabilities and ensure they are using the right tools at the right time and to the right degree. Some examples of tools that – when used in conjunction with feedback loops on the backend – can mitigate the risk of fraud and decrease losses are outline below.

SOLUTION	DESCRIPTION	COMMON USES	SHORTFALLS
Device-Specific Technology			
Digital fingerprinting	Digital fingerprinting allows analysis of a remote device and its characteristics, including installed plugins and software, time zone and other identifying features of the device.	By identifying potentially fraudulent devices, merchants can take preventative measures.	The ability to collect digital or device fingerprints relies on JavaScripting or another client-side scripting language. Users on mobile devices or using privacy software have limited client-side scripting, making it more difficult to fingerprint these users.
Shared device reputation	Sharing the ability to identify fraudsters that have already attacked sites with peers within a system (within and across industries).	The benefit of shared device reputation is the prevention of first-time losses as well as speeding up ROI.	This technique is only effective in preventing fraudsters that have attacked before and not on emerging threats not already stored in the shared database. Sharing this type of information can be seen as aiding competitors.

SOLUTION	DESCRIPTION	COMMON USES	SHORTFALLS
IP-Based Technology			
Proxy databases	A database of known proxies that fraudsters use to hide their IP addresses, and their true locations. Proxy-piercing information via IP address provides non-invasive insight into the risks involved with accepting transactions from specific IP addresses.	Proxy identification is used to detect malicious traffic.	Database must be current for it to be effective.
Geolocation	Geolocation uses digital information via the internet to identify the geographical location of a fraudster.	Geolocation is an effective, non-invasive tool for comparing IP location to registered billing addresses, allowing merchants to identify and block connections that pose a risk or to block specific IP addresses from suspicious locations.	While this forensic information can be used in court, some geolocation tools may be limited in the granularity of data provided.

Fraud Solutions Continued

SOLUTION	DESCRIPTION	COMMON USES	SHORTFALLS
Data Solutions			
Customer Validation	Customer validation uses consumer data from various public and private sources to validate the billing information associated with the payment type.	Customer validation can happen at multiple levels including checking a billing address via an Issuer to validate full name, address, phone and email.	Validations are limited capabilities of the provider and leveraging more detailed solutions can be expensive.
Identity verification	This type of tool can be used to verify and validate a person's identity based on information they enter such as name, address, date of birth, country specific ID (i.e. SSN) and phone.	Using identity verification, specifically for merchants with high-value transactions or those involved in age-restricted industries such as alcohol, tobacco or gaming can help prevent instances of identity fraud.	If not automated, this technique can hinder the customer experience by slowing transaction speed. Additionally, asking for PII (personally identifiable information) can be seen as invasive and customers are hesitant to add this information to an e-commerce transaction.
Knowledge based authentication	Knowledge based authentication for high-risk CNP transactions involves a user answering a question that cannot be found in a wallet or online (prior residences, mortgage amounts, etc.).	This type of authentication is often used in high dollar amount transactions or age-restricted industries to verify a user's identity.	This requires a user to remember potentially obscure pieces of personal information and can extremely impact the overall user experience since this authentication occurs after an identity verification.
3D Secure	3D Secure is an additional authentication step for CNP payments. Visa developed this XML-based protocol to improve the security of Internet payments.	This protocol is used as an additional security layer for online credit and debit card transactions.	Places an inconvenience on the customer by adding authentication step during the sales process. Abandonment rates may increase when customers see the 3D logo by Visa or Mastercard.[64]

SOLUTION	DESCRIPTION	COMMON USES	SHORTFALLS
Mobile-Based Technology			
Mobile secure location	This tool is a data point allowing for verification of a cardholder's mobile location during post-transaction review, allowing for the identification of actual fraud cases and the reduction of false positive administrative costs.	This data point reduces cardholder service interruptions, resulting in optimized customer experience.	Secure location is dependent on mobile phone availability and is an out of band fraud prevention.
Identification and isolation of suspect transactions	Using radio environment examination captured by a customer's mobile device during the transaction, merchants can gather information about Wi-Fi access points in the area, verified GPS information and IP address information.	This information is processed on a secure server, which examines signals to obtain a location estimation via Wi-Fi access points, cell towers and geolocated IP addresses.	This solution is post-transaction completion and does not prevent the fraud before it happens.

Fraud Solutions Continued

EMERGING SOLUTIONS		
SOLUTION	**DESCRIPTION**	**COMMON USES**
Biometrics	This solution uses keystroke analysis, fingerprinting, voice, iris and facial recognition technology to identify and validate people.	Has expanded the ability for businesses to authenticate a person's identity using components other than simple data points like name, address, location.
Email verification	This emerging solution associates email address with an individual and/or address. Some technologies leverage algorithmic, linking technology to evaluate an email provided with order information, name, address, and phone number providing a fraud score for decisioning.	Authenticates that an email address being used in a transaction is associated with the name and address provided.
Social media validation	This is a Profile-based solution that can be looked up via SM "token" or email address and allows for a way to validate an individual's personal information.	This solution can provide a secondary way to validate real customers, including millennials, unbanked persons, non-U.S. customers and the younger demographic. These users cannot typically be validated by traditional Know Your Customer processes. Linking attributes to multiple identities reduces false positives while providing a reduction in manual reviews.

Cost of Overprotection

While employing every single fraud prevention tool available is neither feasible nor necessary, merchants should be aware of the types of solutions available and employ each as needed. In the end, merchants need to evaluate the cost of fraud prevention against the benefits. It's easy to fall into the trap of "turning on" all fraud prevention measures to ensure that nothing seeps through the cracks; however, there is such a thing as being too aggressive. Having a 0.00% chargeback ratio is not a desired outcome if you are turning away 10% of your good customers in the process. A balance needs to exist between what you are turning away and what you accept as valid.

When fraud-scoring tools are too sensitive, the result is an unnecessary amount of false positives, causing card declines for legitimate purchases. There can be as many as 40 false positives for every legitimate attempt at fraud, **meaning that up to 97% of transactions flagged as high-risk can be legitimate transactions.** These false positives result in card declines, significant sales loss, blocked accounts and overall poor customer experience.[65]

The next chapter will discuss how effective post-sale management operations can limit the sales impacts born of overly conservative upfront fraud prevention.

40 false positives  **attempts to fraud**

97%
of transactions flagged as high-risk
are legitimate transactions

Big Data – A Blessing and A Curse

Data Breach Risks 2013 and 2014 saw a rash of data breaches, illuminating the fact that, as businesses continue to use consumers' personally identifiable information (PII), there is more sensitive data at risk of being used by fraudsters. Currently, 47 states have active data breach laws that require notification by the affected parties to help consumers take the necessary actions to protect themselves. Despite numerous laws and safeguards, breaches continue to occur. The impacts these breaches have to businesses are grave: 60% of breach victims report a significant decrease in amount of trust they have for a retailer who has been breached.[66] Only 10% of breach victims reported that they were confident in that merchant's ability to protect their PII in the future.[67] Roughly 20% of victims say they would avoid doing business again with breached merchants.[68]

The mega retail breaches of the past few years have brought to light numerous vulnerabilities that need to be addressed. Merchants have faced consumer lawsuits as a result of these security breaches and should expect that more stringent federal regulation will result in an attempt to protect sensitive PII data. Only about 25% of consumers believe health care and financial data are sufficiently protected by current federal data security requirements, indicating legislation calling for greater accountability by organizations may be on the horizon. Merchants must also take into account the cost of fighting and potentially losing consumer lawsuits as a result of data breaches.[69]

Using Big Data to Fight Fraud Big data has been a big buzzword in the payments space and with good cause. Given the dynamic, real-time threats that are presented by fraudsters daily, the need for an analytical solution based on big data is evident. As fraud becomes more complex, analytics will have to adapt at the same pace to remain effective. Using big data as the basis of anti-fraud technology has made payments safer: U.S. credit card fraud has dropped 13 basis points since 1992, from 18 to 5.[70]

Big data is powerful - for every payment card that is swiped or account number entered, fraud prevention tools complete up to 15,000 calculations within milliseconds to determine if a transaction is fraudulent, based on trillions of historical transactions and unmatched intelligence. Analytics of big data enable fraud solutions to intelligently identify patterns and automate the authorization process securely.

In addition to calling on and analyzing historical data, sophisticated modeling can learn and adapt to changing or new patterns, preventing fraud when access to historical or relevant data isn't necessarily available. This self-calibration and adaptive model already happen in close-to real-time, streamlining the fraud prevention process without adding friction to the shopping experience for customers. By self-learning, fraud solutions can become sensitive to recent fraud patterns and create behavior archetypes based upon transactional behavior across millions of customers, providing a more granular comparison of "normal" shopping behavior versus suspicious behavior. This information can significantly reduce false positives and decrease the cost of manual reviews and other operational costs associated with identifying fraud.[71] Some of these advanced tools are outlined below.

Omni-channel Evolution: The Need for a Layered Approach to Fraud Prevention

There is no one "silver bullet" to protect card-not-present transactions from fraud. As omni-channel commerce continues to evolve, the need for comprehensive, strategic and agile fraud prevention measures will be critical to merchants in protecting profits and boosting sales. Forrester projects that cross-channel transactions will reach $1.8 trillion by 2018, boosted by the use of smartphones to research products before purchasing.[72] Research shows that merchants with a solid omni-channel strategy boost sales, but there are disadvantages too. One study reported that 77% of merchants thought multi-channel retail makes fraud prevention more difficult and 76% thought it actually left them more vulnerable to fraud.[73]

As the digital and physical worlds continue to converge, there are steps merchants can take to mitigate omni-channel risks without hurting conversions. The key is implementing intelligent tools and solutions that span across channels and that can be tested and toggled to remain agile and adaptive as new threats emerge. A layered approach to security is absolutely necessary. CNP merchants should cover their bases by leveraging proven technologies to evaluate and analyze the type of fraud you are experiencing. Once determined, leverage multiple fraud prevention methods that address your specific fraud vulnerabilities, while protecting against others. It is important to remember to balance the lever and determine the "acceptable" amount of fraud for your organization without dramatically impacting sales.

Matthew Katz, CEO of Verifi Inc., emphasizes the importance of evolving your fraud prevention systems to keep pace with new technologies and fraudsters. "As the industry continues its growth bolstered by new technologies, merchants will find themselves inundated with new tools and "shiny objects" from which they can choose to protect payments, streamline payment processing and fight fraud. But merchants will not be able to effectively use these new tools without a capable processing environment that is stable enough to withstand today's challenges and agile enough to adapt to tomorrow's threats. Merchants need flexible fraud prevention capabilities that can be tailored to their business and evolve alongside the changing market." A holistic approach to fraud and risk management can decrease losses, increase sales and improve customer service. Fraud is not preventable, but an ongoing investment in fraud prevention can yield dividends and improve bottom line.

Navigating Post Sale Chargeback Challenges

Chapter 3

As mentioned in the previous chapter, effective front-end fraud protection is vital to a healthy CNP business, but being overly conservative can unnecessarily curtail sales and profits. This chapter will explore the concept of total chargeback management as a method for preventing and recovering revenue lost to fraudulent chargebacks.

Chargebacks are a $40 billion problem. In 2014, merchants reportedly lost a 33% greater proportion of revenue to fraud over 2013.[74] In addition to the cost of each chargeback for which they are held liable, merchants are responsible for paying fees to financial institutions – which can balloon to $100 or more[75] – and must also bear the cost of replacing and reshipping lost or stolen goods.[76] These costs can cripple a business.

How Chargebacks Occur

Chargebacks occur when a customer contests a card payment with the issuing bank. They can occur for a number of reasons. Here are some common reasons:

TYPE OF CHARGEBACK	CAUSE
Criminal Fraud	This common type of chargeback occurs when an unauthorized transaction takes place.[77]
Credit Not Processed	This is a common type of chargeback that happens when a customer returns goods to a merchant and requests a refund,and then reports that the credit was not posted to their account.[77]
Item Not Received	This occurs when a customer pays for an item and claims they did not receive it.[77]
Technical Problems	Chargebacks of this sort are related to a technical issue during the payment process. This could be a problem between the issuing bank and the merchant, resulting in a double charge to the cardholder. These chargebacks may also be related to issues during the authorization process.[77]
Canceled Recurring Transaction	Canceled recurring transactions occur when the cardholder notifies issuing bank that s/he asked a merchant to cancel a recurring transaction but the card was still charged, merchant did not notify the cardholder prior to processing recurring transaction per the agreement or the recurring transaction amount was greater than the pre-authorized dollar amount.
Friendly Fraud	Friendly fraud happens when a customer makes a purchase and then requests a chargeback, even though they have received the goods or services they purchased. **There are several friendly fraud reason codes. The first common type of chargeback related to friendly fraud is "Non-Receipt of Goods/Services":** **Visa:** 30 **MasterCard:** 55 (goods) & 59 (services) **American Express:** C08 (May also be coded as 155) **Discover:** RG (May also be coded as 4755) **Another common type is "Canceled Recurring Transaction":** **Visa:** 41 **MasterCard:** 41 **American Express:** C10 **Finally, friendly fraud chargebacks may be due to "Cardholder Does Not Recognize Transaction":** **Visa:** 75 **MasterCard:** 63 **American Express:** FR3

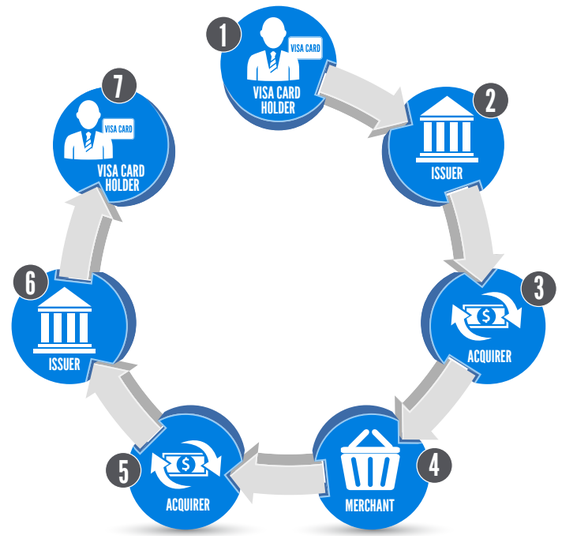
Friendly Fraud - A Growing Problem

Friendly fraud happens when a consumer fraudulently reports a legitimate charge to their financial institution to obtain a refund, leaving the merchant to cover the cost of the goods or services in question as well as related card association fees.[78] While some friendly fraud is accidental (when someone does not realize that a family member has made a purchase using a card or does not recognize the billing descriptor on their credit card statement and reports it as fraudulent), other causes can be buyer's remorse, a sophisticated form of shoplifting or a case of identity theft.

Friendly fraud is so easy that it's costing CNP merchants billions each year; an estimated $11.8 billion in 2012, according to Visa. In addition to being a costly epidemic, friendly fraud has the potential to put CNP merchants out of business entirely; merchants with higher than 1% of charges reversed as chargebacks can lose the ability to accept credit cards altogether.[79]

With the recent breach and theft of more than 100 million credit and debit card numbers from major US retailers, the threat of friendly fraud is at an all-time high.

Chargeback Life Cycle



1. The cardholder disputes a transaction.
2. The Issuer sends the transaction back electronically to the acquirer.
3. Once the acquirer receives the chargeback, it will resolve the issue or forward the issue to the merchant. Merchant can learn of chargeback up to 180 days after date of purchase.
4. The merchant can either accept the chargeback item or dispute and represent. Once addressed, the merchant can resubmit to the acquirer.
5. The acquirer reviews information and supporting evidence received from the merchant. If the acquirer sees sufficient evidence that the merchant has addressed the chargeback, the acquirer represents the chargeback electronically to the Issuer.
6. The Issuer receives the represented item and takes one of two actions:
   a. The Issuer will re-post the transaction to the cardholders account, or
   b. The Issuer may submit the items to the acquirer for a financial liability decision if the chargeback issue is not adequately addressed.
7. Finally, the cardholder receives the dispute resolution information and is either re-billed or credited for the item.[80]

Chargebacks: Common Myths and Misconceptions

Fighting chargebacks can be a time-consuming and resource-draining task for merchants that do not have the necessary expertise. Debunking common misconceptions and addressing common problems in the dispute resolution process provides a good basis for merchants looking to implement a winning chargeback program.

MYTH	REALITY
You can't win CNP chargeback disputes	Employing the expertise of a vendor can not only relieve the time and resources needed to dispute chargebacks and reclaim lost dollars, but some vendors are able to provide net recovery rates of more than 50%, significantly boosting a merchant's bottom line.
Winning chargeback disputes will reduce your monthly chargeback ratio with your acquiring bank	Chargebacks are not reduced if won; once they occur, they count against a merchant's chargeback ratio, even though a merchant may be recovering money.
It's impossible to win a CNP chargeback if you don't have a signed receipt.	Compelling evidence can include a number of items other than a signed receipt, including photographs or e-mails proving a link between the person receiving the merchandise and the cardholder, or proving that the cardholder disputing the transaction is in possession of the merchandise.
You can't lower your chargeback ratio without reducing sales	There are a number of steps merchants can take to lower their chargeback ratios without reducing sales. A common method is requiring customers to register their cardholder information (validated by answering a number of questions to which only Issuers and the cardholder know the answers and selecting a secret phrase and password).This feature allows online merchants to validate return visitors in a simple, non-intrusive manner, preserving legitimate sales.
You can't fight PayPal Disputes	PayPal offers Seller Protection from chargebacks to merchants who meet the eligibility requirements based on Unauthorized Transactions or Item Not Received. The scope protects Sellers for the entire amount of payment and also waives the Chargeback Fee, if applicable.

As illustrated in the previous sections, chargebacks happen for various reasons. The reasons for occurrence, risk of occurrence and types vary widely depending on the billing model of the merchant. Chargebacks can occur on one-time purchases or on recurring purchases and it is important to understand the ramifications – as well as the different preventative measures – each scenario entails.

Chargebacks: An Ounce of Prevention

Preventing chargebacks is essential to stopping unnecessary revenue loss and merchant account problems. There are several basic practices merchants should follow to reduce chargebacks.

This starts with improving internal operational measures to limit the opportunity for chargebacks to occur:

- **Be proactive** Monitor chargebacks to analyze where there is room to take preventative measures. By tracking chargebacks by reason code, merchants are able to tie these reasons back to a specific remedy and incorporate the necessary preventative measures.
- **Separate initial chargebacks from chargebacks that stand after representment** By looking at the ratios of unresolved chargebacks post-representment, merchants can evaluate the effectiveness of representment procedures unrelated to supporting documentation. A high proportion of net chargebacks that are not reversed points to a need for review of sales and order process and customer correspondence.
- **Implement additional fraud controls** According to Visa, there are several actions a merchant should take to prevent fraudulent chargebacks before they occur:[81]
  - Monitor IP address and account number velocity
  - Place restrictions on IP addresses with a history of previous fraud.
    - IP addresses with a history of fraud-related chargebacks or other fraudulent transactions should be blocked.
  - Only allow a certain number of payment cards to be linked to a single IP address.
  - Limit the number of times a card can be used or set up flags per the number of transactions made with a card during a specific time period (24 hours)
  - Prohibit the same card from being used to make payment on more than "X" number of different accounts
  - Monitor accounts with excessive usage
  - Monitor high-value transactions

Single Sale vs. Recurring: Preventing Chargebacks

BILLING MODEL	CAUSE	PREVENTATIVE MEASURES
Single Sale	• Information requests from cardholder's bank. • Processing error: transaction processed multiple times resulting in multiple charges. • Refund not processed. • Invalid account number. • Transaction not processed timely. • Simple billing error (overcharging).	• Offer quality products • Offer clear descriptions of products and services • Post an anti-fraud statement on merchant website • Maintain clear records of sale, including transaction logs, receipts, and CVV/AVS audit trails. • Provide ample customer service, including telephone numbers, email addresses and chat communication for customers. • Use clear billing descriptors. • Use AVS & CVV verification. • Provide status updates for delayed shipment of orders. • Enact clear and quick refund policies.
Recurring	• The card Issuer may have canceled the card account or charged back a previous recurring transaction. • The cardholder may have withdrawn permission for the merchant to charge the account, canceled payment on a membership fee or canceled the card account. • The merchant exceeded the pre-authorized dollar amount without notifying the cardholder prior to the date of the transaction, notified the cardholder in writing within ten days of the recurring transaction without receiving consent from the cardholder, or received notice that the cardholder's account had been closed. • Failure to render services • Refund not processed. • Invalid account number. • Transaction not processed timely. • Simple billing error (overcharging) • Does not recognize charge after original order, resulting in multiple chargebacks for multiple recurring charges since origination.	• If the transaction was canceled and a credit was issued to the cardholder, merchants should inform the acquirer of the date the credit was issued. • If the transaction was canceled but the customer still received the goods or services, the merchant should supply proof to the acquirer that the customer used the goods or services between the date of the previous billing statement and the date of the requested cancellation. • If there is evidence that the cardholder expressly renewed the services contract, evidence of the renewal should be supplied to the acquirer. • When a customer cancels recurring payments with a final payment still due, merchants should contact the cardholder directly for payment rather than automatically billing the customer, to avoid potential misunderstandings. • Merchants should handle customer cancellation requests in a timely manner and be sure to follow up with a notification to the customer that their recurring payment account will be closed. • Process credits promptly. Cancellation requests received on the cusp of upcoming recurring payment transaction dates often result in an unnecessary charge and a credit should be posted to the cardholder right away, along with a notification that the credit has been issued. The following chapter will explore recurring billing in greater detail. • Merchants should send out monthly (bi-monthly, yearly, etc.) reminders prior to sending out the bill or charging a customer's account. These reminders can be helpful to consumers who may have forgotten about a recurring charge and help to prevent chargebacks from 'Cardholder does not recognize transaction.'

Proactive Customer Service Can Help You Avoid Chargebacks

- Maintain consistent customer service hours and be sure that they are posted in an easily visible place on your website.
- Set up clear refund policies and ensure they are honored in a timely manner.
- Optimize response times to retrieval requests and chargebacks to portray the sense of “instant gratification” to consumers.
- Make it “easy” for the consumer to connect with you. Skimping on email communication or live phone support access will cause more problems in the long run.
- Utilize call centers or IVR systems to provide weekend and off-hour support so customers have access to you 24/7.
- Augment customer service with support via website, email & Live Chat and enable consumers to easily contact you, decreasing potential frustrations caused by inaccessibility.
- Remain in contact with consumers when appropriate. A friendly email reminder of an upcoming recurring bill payment can decrease confusion as to why the consumer was charged.

Chargeback Management – Recovery

Even if you’ve instituted comprehensive chargeback prevention measures both internally and with external tools, chargebacks can and will happen. Verifi’s research showed that 86% of the time cardholders will not contact the merchant until after a dispute was filed...or not at all! Chargebacks are a part of doing business for CNP merchants. The rules are always changing. Most recently, the rules for Reason Code 83 shifted, allowing merchants more leverage in fighting friendly fraud.

So how does a business recover lost revenue from chargebacks? There are several strategies a merchant can employ to reduce the operational (and often hidden) costs of chargebacks:

OPERATIONAL EFFECTIVENESS

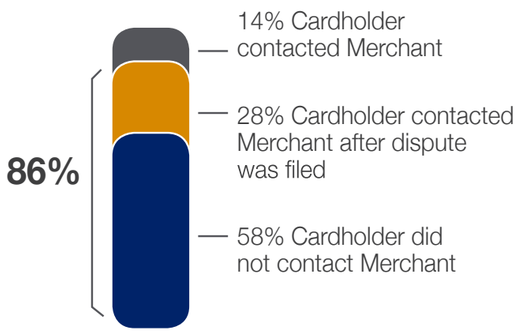
- **Automation** Streamlining workflow and eliminating human error reduces the time and resources needed to process a chargeback. Automation also allows for merchants to remain current on credit card processing rules and make the dispute process much simpler.
- **Data control** Collecting information from chargebacks allows the merchant to adjust business practices if necessary and identify internal issues.
- **Chargeback tolerance** It makes no sense to spend more disputing a chargeback than one would incur in chargeback fees. Things to consider when a chargeback occurs:
  - What is the cost of the chargeback to my business?
  - What is the cost of fighting the chargeback?
  - What is the probability that the business will be successful in the dispute?

WAYS TO MANAGE DISPUTES

- **End-to-end software solutions** This goes hand-in-hand with the automation process in that it allows merchants to bundle all the necessary chargeback processes into one platform. Businesses should invest in software that handles all aspects of the chargeback process, from analysis to reporting.
- **Improve the process** Streamlining workflow and eliminating human error reduces the time and resources needed to process a chargeback. Automation allows for merchants to remain current on credit card processing rules and make the dispute process much simpler.

- **Prioritize** Businesses should have a fight or flight policy built into the chargeback process. It makes no sense to spend more time disputing a chargeback than one would incur in chargeback fees.
- **Make your evidence compelling** When disputing a chargeback, it is important to provide documentation between the cardholder and the merchant that proves the merchant communicated with the cardholder and that the cardholder knew about the transaction.
- **Transaction based support** If you can prove that the merchant swiped or imprinted the card and received an authorization approval and the cardholder's signature, it is much easier to receive a favorable decision.
- **Identity based support** To recover funds lost from the chargeback process, the best way for a merchant to contest a chargeback is to give the bank evidence that proves the transaction was authorized and the identity of the customer is the same as the cardholder. This is done by providing evidence usually captured in a merchant's CRM such as:
    - Customer identity (PII data- email, address, physical address, name, DOB, etc.)
    - Purchase history and usage information
    - Contact history (email/phone communication)
- **Get outside expertise** Tasking a third party with all or some of the chargebacks allows the business to free up resources and valuable time that can better be spent running a successful enterprise. Additionally, employing a third party that is experienced in dispute research and support and who has established relationships with processors, Issuers and banks allows for seamless transmission of chargeback data. In aggregate, these can ensure higher funds recovery and faster and efficient resolution.

Verifi's research showed that 86% of the time cardholders will not contact the merchant until after a dispute was filed...or not at all!



Tips for Fighting PayPal Disputes

PayPal offers Seller Protection from chargebacks for eligible merchants who meet certain requirements, depending on whether the merchant is seeking coverage for Item Not Received or Unauthorized Transaction.

ELIGIBILITY REQUIREMENTS

The basic requirements for Seller protection mandate that the item be shipped to shipping address on Transaction Details Page with sales documentation provided in a timely manner and the Seller's primary residence must be in the United States. Additional requirements for protection by dispute type include:

- Payment must be marked "eligible" (Unauthorized Transaction Coverage) or "partially eligible" (Item Not Received Coverage) for Seller protection on Transaction Details page for Chargeback protection
- Merchant must provide Proof of Delivery (Item Not Received Coverage) or Proof of Shipment (Unauthorized Transaction Coverage)
- Pre-ordered and made-to-order goods should be shipped within the timeframe listed in item listing or within 7 days after receipt of payment (Item Not Received Coverage)[82]

PayPal™

Merchant Issuer Collaboration – A Win/Win for Everyone

Chargeback disputes are a costly process for Issuers and merchants alike. Both parties face increased pressures from market forces - increasing regulations squeeze the margins of Issuers and the increased cost is passed down to merchants. When it comes to chargebacks, the default is for merchants and Issuers to act as separate entities; however, this disconnect between Issuers and merchants is expensive. Lack of communication means transactions suspected as fraud and cardholder initiated disputes snowball into chargebacks rather than potentially being avoided through Issuer/merchant cooperation, processing a refund or issuing a credit and ultimately resolving the dispute upfront.

Fraud management for CNP payments has always been essential, but as fraud and chargebacks rapidly increase, it is more crucial than ever for merchants and Issuers to work together to mitigate CNP risk. Cardholder dispute behavior puts both merchants and Issuers in a bad position. 58% of cardholders don't contact the merchant at all when filing a transaction dispute, and another 28% contact the merchant after the dispute had already been filed. When cardholders bypass the merchant and contact the Issuer directly, you lose time and money. Disputes are expensive to manage and write-offs and arbitration are costly – arbitration cases alone can cost $250 to $750 per case.[83]

Chargeback dispute notifications facilitate better and timelier communication between Issuers and merchants who are part of a collaborative network facilitated by a service provider. This network lets Issuers notify merchants of pending disputes, empowering the merchant to resolve the dispute directly with the consumer. By communicating before a dispute is processed as a chargeback, merchants have the opportunity to resolve the issue and process a refund or issue a credit so that a chargeback never occurs.[84]

Real time data sharing between merchants and Issuers aid in the fight against fraud. Issuers can provide these real time alerts to notify merchants the likelihood of a chargeback result is high. Rather than immediately filing a chargeback when a customer dispute is filed, the Issuer notifies the network service provider, which passes the data to merchants who can then resolve the dispute directly with the cardholder. The benefits for both Issuers and merchants include decreased operational costs, better customer experience and improved bottom line, in addition to:

MERCHANT	ISSUER
INCREASED EFFICIENCY — More efficient use of resources and staff - chargebacks are expensive because the dispute resolution process is complex, time consuming and labor intensive. The expert level of understanding required is significant. Manual processing, reconciliation and reporting as well as interaction with various banks often results in inefficiency - some of which may not always be evident on the balance sheet.	**HIGHER EFFICIENCY** — Rather than dumping time and staff into resolving extensive disputes, Issuers can automate the dispute resolution process and resolve disputes quickly.
MORE EFFICIENT USE OF RESOURCES AND STAFF — Near real-time notifications alert merchants of chargebacks immediately, enabling quick resolution without draining resources and staff to the exhaustive chargeback management process.	**REDUCED OPERATIONAL BURDEN** — Properly filing chargebacks with the correct reason codes and documentation is time-consuming. Issuer alerts eliminate the need for this by allowing the Issuer to pass the dispute to the merchant to handle directly.
ELIMINATE CHARGEBACK FEES AND PENALTIES — Collaboration allows for the prompt resolution of disputes before fees and penalties can be imposed.	**BETTER CUSTOMER EXPERIENCE** — By using alerts to bring the merchant back into the loop and communicate directly with the cardholder, the customer wins. When disputes are handled internally by Issuers, it may lead to lags in response time, lack of timely access to critical documentation and other problems. Issuer alerts cut down on attrition due to bad customer experience.
AVOID ADDITIONAL LOSSES OF GOODS AND SERVICES — Merchants rarely receive back the original merchandise or service provisioned, adding to the total amount of losses. Organizations with a recurring business model or subscription services must also take into account services rendered when chargebacks occur, as these non-tangible goods cannot be returned.	

How Outside Expertise Can Help

Reducing losses from unwarranted chargebacks requires internal measures and, more often than not, the expertise of a third party to establish controls appropriate for your business environment. Whether you're completely outsourcing or just augmenting areas that you cannot completely do in-house, working with a vendor can bring relief to some of the major challenges merchants face:

- Fighting chargebacks in-house is time consuming and expensive and often results in the inefficient use of internal resources.
- Often businesses attribute disputes as a cost of doing business that can add additional losses related to excessive refunding or lost merchandise that never gets returned.
- Knowing when to dispute the chargeback and the complex and changing rules and reason codes takes deep expertise and insights to maximize results.

Because of the costs and time investment required for preventing and fighting card-not-present fraud, it's important to carefully consider how you select a third-party vendor to aid in chargeback prevention and recovery. For merchants that only need to outsource a part of their prevention or representment requirements, a vendor can help streamline the process so you can focus on your core business while lowering the operational costs associated with chargebacks.

The most effective solution is to find a vendor that closes the need gap and decreases costs and man-hours.

NEED	SOLUTION	RESULTS
Reduced chargeback volume	Identify a provider that broadly covers the vast number of chargeback reason codes with the flexibility to fully manage the resolution process or provide self-service options.	Lower realized chargeback volume and improved chargeback ratios and stability of bank processing capability. Less dependency on upfront fraud screening which may negatively impact sales.
Improved chargeback dispute resolution process	Look for a provider with established processor and direct and integrated Issuer relationships.	Direct Issuer integration avoids "false positives" and over-refunding. Seamless and timely receipt of chargeback data helps avoid additional chargebacks and shipping of merchandise/provision of services to fraudsters.
Measurable ROI	Find a provider with a flexible, pay-for-performance model and established track record of identifying which chargebacks warrant dispute and a proven recovery rate success.	Avoids frivolous time waste and fosters better Issuer and Merchant collaboration. Clear success path. Avoids paying for time and labor without known return. Historical win rates provide better internal revenue and earnings forecasting.
Reduced man-hours wasted on non-core activities	Look for an experienced team with seamless workflows that are directly connected with card Issuers to speed up resolution and recovery.	Improved utilization of internal resources toward core business, reduced cost, and improved cash flow.

Benefits of Total Chargeback Management

Total chargeback management requires merchants to take into consideration a number of risk management strategies. Regardless of whether or not you choose to implement some or all of these strategies, it is imperative to take the toll of chargebacks into consideration. With each chargeback comes the burden of cost that can rack up significantly. Take the example below. If we assume 1000 chargebacks per month with an average purchase price of $50 and an additional $50 in fines, fees and other costs associated with each chargeback, we see how quickly the costs stack up:

CHARGEBACKS PER MONTH	1000
Average purchase price	$50
Other costs associated with managing chargebacks (fines, fees, time, etc.)	$50
TOTAL COST OF CHARGEBACKS	**$100,000**

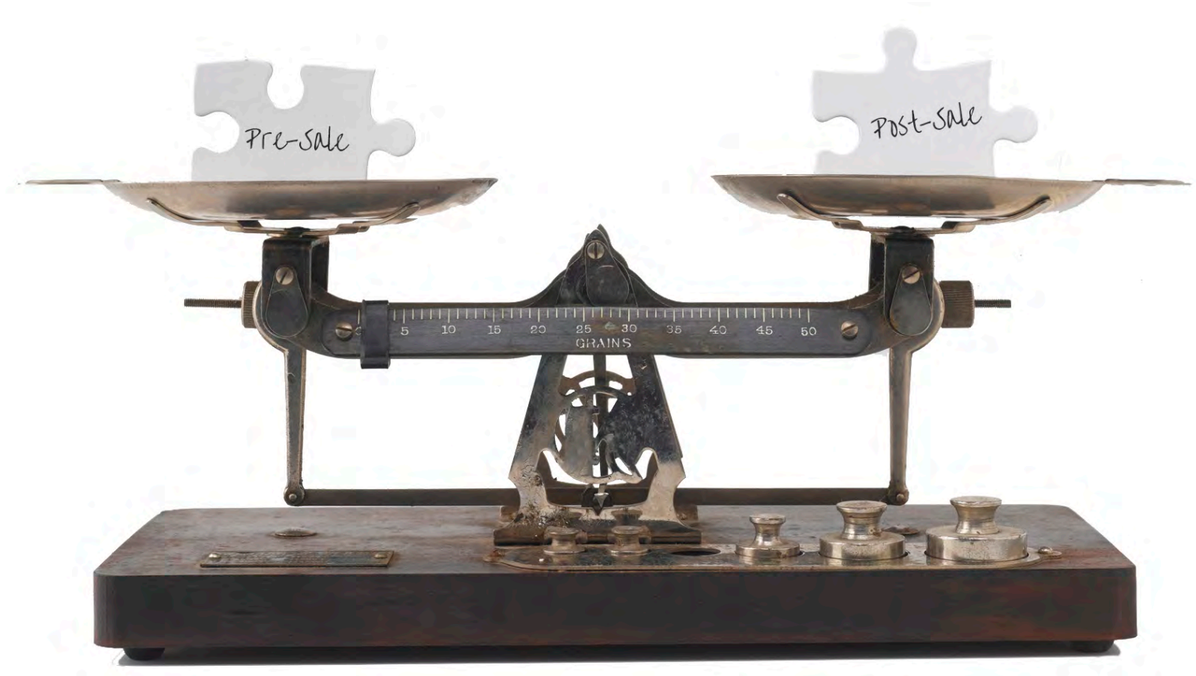
At the rate above, if a merchant is able to achieve a chargeback avoidance rate of 30%, the savings total $30,000. In taking it a step further, successfully representing 50% of unavoidable chargebacks results in additional savings of $35,000, significantly improving profit.

IF...	
You prevent 30% of your chargebacks	**$30,000** Saved
You successfully represent 50% of the remaining chargebacks	**$35,000** Saved
TOTAL SAVINGS	**$65,000**

In addition to impacting profits, excessive chargebacks may also indicate problems in operations. Whether it is a quality control issue with merchandise, ineffective or misleading product marketing or another root cause, identifying and addressing these issues can significantly reduce the occurrence of chargebacks. Your business should conduct an analysis to identify points of failure. Not only will you reduce the impact of chargebacks on profit, but also your customer satisfaction will increase.

Trade Offs of Pre-Sale vs. Post-Sale

In this chapter, we've outlined total chargeback management, including understanding the reasons why chargebacks occur, operational process improvements to aid chargeback avoidance, managing unavoidable chargebacks effectively and recovering lost funds. This section also illustrated how great post-sale prevention and mitigation can allow merchants to loosen up front-end fraud tools to minimize lost sales from preventing validated transactions and provide a less disruptive customer experience. The following chapter will delve deeper into the recurring billing model and the impact of churn and will also touch upon some alternative billing models and best practices.



Maximizing Your Billing Efforts and Customer Retention

Chapter 4

Maximizing credit card acceptance for a CNP merchant is vital to profitability and longevity of the customer relationship, especially in recurring models. This section explores the different types of billing arrangements and various payment considerations for recurring, installment and negative option program as well as best practices for managing each type of billing model.

Why Cards Decline

The historic data breaches of 2013 and 2014 were no laughing matter; the Target breach affected more than 70 million customers and the Home Depot breach compromised more than 56 million payment cards.[85] As a result, banks re-issued millions of credit and debit cards, resulting in unnecessary payment declines due to outdated account information. New replacement cards and additional scrutiny are increasing unintentional payment decline rates for merchants with recurring subscriptions services such as apps, cable television, software, cell phones and other industries. In addition to a loss of billings, merchants are seeing a loss of customers. The top of mind question is: "How do I recover these losses?"

Maximizing Payment Card Acceptance

Payment card brands have increasingly been launching new products tailored to certain demographics, including electronic transfer (EBT) cards, rewards cards and prepaid cards. With these new products, more data has been introduced into the payment life cycle. This data has increased challenges in authorization management but has also created new opportunities for increased profitability. Improving billing and authorizations requires a secure payment processor that acts as a partner to aid in seizing these new opportunities and mitigating risk.

Much of this new available data is passed along to payment processors via the purchase authorization response, though because of the complexity and uniqueness of the data sets, some processing platforms do not have the capacity to adequately capture the data. This unique data has become an important differentiator for merchants and subsequently, for payment processors who are able to pass data in the authorization response. This enables merchants to better engage with customers via merchandising and retention strategies.

In the prior sections, we talked about safe and secure processing, proper customer authentication and optimizing your billing yield. Customer retention is an important part of optimized billing and relies upon the minimization of unnecessary card declines.

Any business that depends on monthly recurring revenue will see churn from unwanted credit card errors. Losing customers is bad; losing customers that want to continue paying you is especially painful.

DID YOU KNOW?

Just 20% of existing customers will be responsible for 80% of future profits, according to Gartner Group.[86]

There are a number of reasons that cards decline, some of which can be prevented:

- Expired card accounts have not been updated
- Timing of the authorization
- Processing errors related to the authorization message

Look at the authorization decline response codes - This message should come from your payment gateway and may offer additional insight into why a transaction declined.

Payment gateways should provide an error code along with a directory of error codes for merchants to reference as supplemental information to error responses. Cards decline for a variety of reasons, resulting in error categories, including communication errors, merchant errors, fraud prevention declines, soft declines and hard declines. Soft and hard declines occur frequently and we've outlined their causes and some examples in the following section.

Soft vs. Hard Declines

Most hard declines require action on behalf of the issuing bank or cardholder before the outstanding issue will be resolved, making subsequent authorization attempts unlikely to succeed. Reasons for hard declines include "card stolen," "invalid card" or "account closed."

Soft declines are transactions that may be successful with a subsequent attempt. Reasons for soft declines include "insufficient funds," "processor declined," or "voice authorization required." The industry standard is to reattempt the transaction up to three times over a number of weeks. It is also recommended that merchants reach out to the customer - especially in the case that subsequent authorization attempts fail - to obtain an alternate form of payment.

The major difference between the two types of declines is that soft declines can be resubmitted one or two days after the decline occurred in an attempt to obtain a valid authorization. Hard declines should not be retried because the reason for the decline is not temporary as in a soft decline; this type of decline is not likely to be successful with subsequent retries. Understanding the types of declines and the different implications between them allow merchants to operate within an acceptable decline ratio.

TOOLS OFFERED BY VISA AND MASTERCARD

Visa and MasterCard offer a number of tools to merchants to improve authorizations, prevent declines and help CNP merchants protect revenue:

Visa Account Updater The VAU helps merchants avoid declined transactions or interruptions to recurring billing due to invalid customer data by allowing Issuers, acquirers and Visa merchants to exchange the most up-to-date customer data.

Recurring Payment Indicator (RPI): RPI is a scoring method that Visa requires to be present in all authorization and clearing records. The RPI allows for the identification of recurring transactions as well as more accurate decision-making by Issuers. Because recurring transactions tend to be lower risk transactions as compared to single occurrence CNP transactions, they should be approved as long as the account is in good standing.

Address Verification Service AVS helps high-risk merchants protect CNP revenue by verifying a Visa cardholder's billing address with the Issuer.

Card Verification Value 2 CVV2 is a three-digit number found on a Visa card used by merchants to verify that the customer actually possesses the card being used in a transaction.

Verified by Visa® This service provides verification and validation of a cardholder's ownership of an account in real time by prompting customers to enter a password used to confirm the cardholder's identity by the Issuer.

Payment Card Industry Data Security Standard The PCI DSS is comprised of twelve security requirements to protect cardholder data. This standard was created by Visa to provide merchants with consistent data security protocol.

Canceled Recurring Payment Transaction This MasterCard service allows acquirers, Issuers and merchants to avoid costly chargebacks by allowing Issuers to block erroneous recurring transactions in the MasterCard authorization system, eliminating the charges from cardholder billing statements.

Decline Management and Customer Retention

Churn is a problem – an *expensive* one that can cost millions of dollars to your bottom line. Merchants should scrutinize the variables that cause customers to leave. This enables executives to predict and counter churn and maintain - if not boost - profitability. Taking a profit-centric approach allows companies to prioritize each vulnerable customer while considering the profitability of each customer in order to determine what action to take; in some cases, it is more profitable for a low-return/high-cost customer to churn.

CNP merchants with recurring payment business models see higher frequency of declined transactions - up to 25-30% more[87] - and many merchants find that their current decline recycling process is not up to the challenge. By following best practices and using tools that minimize unnecessary and erroneous declines and help optimize billing authorization rates, these merchants can recover revenue that might have otherwise been uncollectable and lengthen the retention of their customer base.

The Economics of Churn and Decline Recovery

Churn is a problem for any company with a recurring billing model; profitability relies on receiving timely, recurring payments. A change in churn rate as little as 1% can mean a difference in millions of dollars to the bottom line.

Merchants should have a basic understanding about churn and its impact on business. Additionally, it is important to understand that churn not only happens when a customer comes up for renewal, but it also happens much earlier in the customer lifecycle. Simple reasons (such as a incorrect credit card number or expiration date, insufficient funds, credit card rejecting an international charge, or other technical issues) are as much to blame for churn as a cancellation. A negative churn rate negatively impacts profitability and valuation.

Decline salvage and recycling programs can improve overall conversion rates. Take, for instance, the example below:

If a merchant has 10,000 current subscribers and the average monthly invoice at $50, that merchant will recognize $500,000 in revenue each month from the recurring base, if successful on all billings. If we assume an average decline rate of 20%, and take into account a range of possible success rates through the decline salvage process, the numbers speak for themselves.

Profit Improvement at Various Decline Salvage Rates

	$ Value of Declines per month at 20%	5%	10%	25%
Monthly Benefit	$100,000 per month	$5,000	$10,000	$25,000
Annualized Benefit	$1,200,000 per year	$60,000	$120,000	$300,000

These conservative recovery rates alone illustrate the potential revenue that can be reclaimed, not to mention the lifetime value that can be salvaged for each customer retained and recovered.

DID YOU KNOW?

A change in churn rate as little as 1% can mean a difference in millions of dollars to the bottom line.

Payment Process Optimization by Billing Type

Card-not-present merchants experience the flux of many variables within the payment life cycle; one of these variables is the type of billing model involved. Seamless execution of each type of billing model requires knowledge of and adherence to industry standards and awareness of the relevant considerations. This section outlines the most prevalent billing models and includes some of these considerations as well as meaningful guidelines for the optimization of each.

RECURRING BILLING

Recurring billing – sometimes referred to as subscription billing – refers to the payment option for customers to pay for a product or service at periodic intervals on an ongoing basis. Some examples of recurring merchants are those that sell magazine subscriptions, ongoing web services (SaaS providers), or products that ship monthly. Recurring billing is a convenient, pay-as-you-go model that can streamline continued business for merchants, though it does require a prudent level of operational efficiency as compared to single-time payments. By implementing industry best practices, CNP merchants can decrease card declines and optimize their recurring billing process.

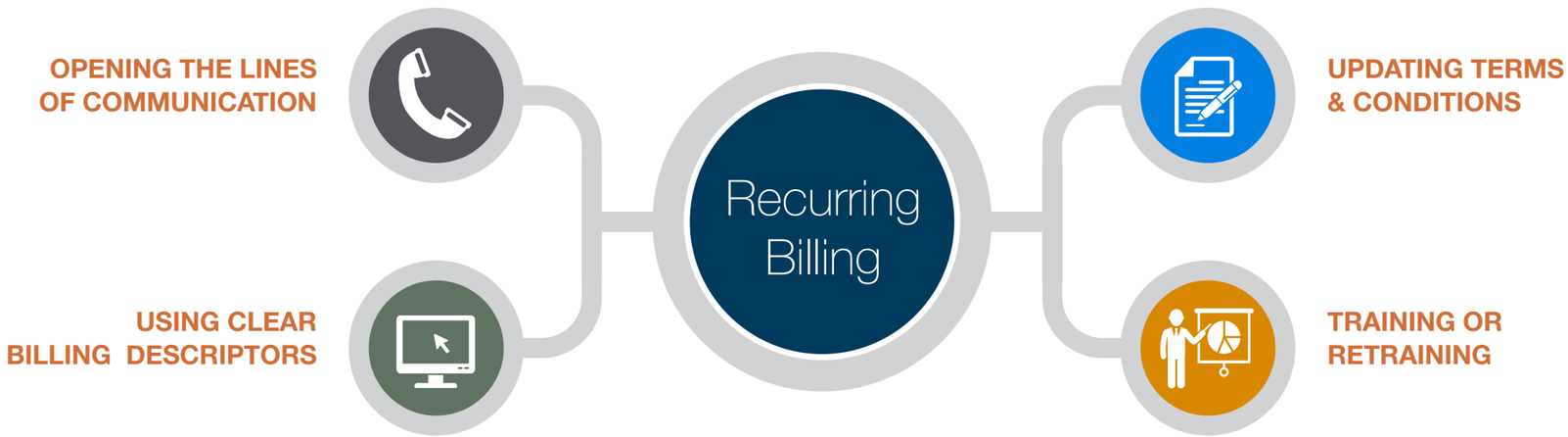
According to MasterCard, decline rates for recurring card billings average a startling 25-30% – that adds up to a lot of lost revenue from customers who don't want to stop paying for your goods or services. Add to that the fact that customer acquisition is 5-10 times more expensive than retaining customers and there is a good business case for effective decline management. By implementing industry best practices, CNP merchants can decrease card declines, optimize their recurring billing process and boost revenue from retained customers.

1. **Opening the lines of communication** Customers should be able to easily locate a toll-free phone number, email address and procedures for canceling transactions via the merchant website or directly on the bill.

2. **Using clear billing descriptors** One of the leading causes of chargebacks is unclear billing descriptors that appear suspicious to cardholders. Any reference to a merchant's URL or website should direct customers to a trove of information about directly contacting the merchant to resolve disputes. This prevents chargebacks and allows the consumer to work directly with the merchant to resolve billing issues.

3. **Updating terms & conditions** Policies should be upfront, understandable and easy to locate. It may be beneficial to rewrite or edit terms and conditions or even include a feedback form to gain consumer input on what a merchant currently has in place.

4. **Training or retraining sales and customer service** Recurring billing transactions can be a sore spot for consumers who feel wronged within the process. By ensuring that customer service and sales departments are well versed on company policies and procedures and able to communicate effectively with consumers on how to resolve issues or disputes, merchants can avoid costly chargebacks and other customer service issues.



NEGATIVE OPTION PROGRAM CONSIDERATIONS

Negative option billing is a model that includes goods or services that are provided automatically wherein the customer must pay for the service or specifically decline it in advance of billing. Because of the potential contentions that arise from this billing model, there are industry standards that merchants should follow when using this billing option.

- **Implement AVS** Transactions where there is "Zip Code Does Not Match" for the AVS response should be declined.
- **Implement CVV 2** Transactions where there is "No Match" for the CVV2 code should be declined.
- **Require additional opt-ins** Items like shipping insurance should not be auto-selected and must require additional opt-in from the customer.
- **Bill shipping and handling charges as part of the recurring charges** These should not be billed separately.
- **Do not use misleading marketing tactics** Card associations do not allow the use of marketing that implies the product is "free."
- **Use clear communication** with customers as to the timing of charges and implement reminder notifications prior to billing with the option to cancel their account.
- **Trial period for a product or service should not require a customer's credit card information** The merchant should send a reminder email near the end of the trial period requesting this information if there is a charge to continue receiving the goods or services after the trial period.

INSTALLMENT BILLING

Installment billing is a popular form of recurring payment. With installment billing, the recurring payments typically occur during a fixed time period, allowing for the cost of a good or service to be broken down into several smaller payments. The following tips can be helpful when processing installment payments:

- **Let the customer choose the billing date** to allow customers more flexibility and better plan how their funds will be withdrawn.
- **Be clear with billing descriptors** and ensure they are set up correctly with your payment processor and will not confuse the customer.
- **Make it easy for customers to cancel** and clearly post the cancellation policy on your website. Clearly communicating the purchase agreement can aid in minimizing disputes and chargebacks.
- **Send email confirmations and billing reminders** prior to processing each payment.
- **Use AVS and confirm the CVV2 Code** when processing the first payment to confirm the validity of the billing address as well as the security codes of CNP payments.
- **Open the lines of available communication** for customer service issues and cancellation requests. Your website should contain a customer service number prominently.

The Future of the Payments Industry

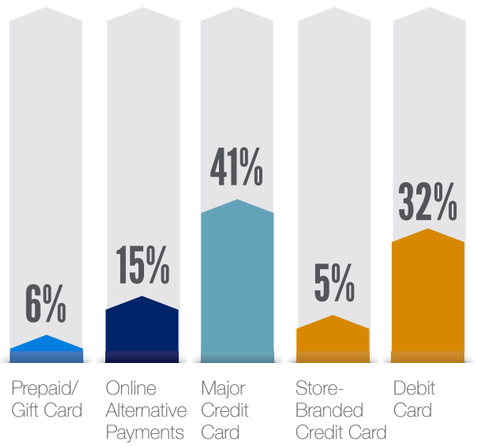
EMV, MOBILE WALLETS, BIOMETRICS AND THE BLURRING OF ONLINE AND OFFLINE COMMERCE

This eBook has discussed the basics of effective payment processing, fraud and risk management in the pre-sales timeline, navigating post-sales chargeback challenges and optimizing authorizations and billing. Looking ahead, EMV will significantly impact both CP and CNP commerce, almost eliminating fraud within the former and aggravating it in the latter. Compounding this trend is the emergence and growing popularity of mobile wallets, which utilize the EMV-compliant NFC technology to let consumers make proximity payments with their smartphones. As fraud moves to the online channel and omni-channel shopping increases, merchants will need a multi-layered fraud prevention strategy that protects payments from end-to-end without stopping legitimate sales from getting through.

Biometrics is another field that continues to evolve as a means of authentication in payments. We see it with Apple Touch ID, the authentication feature used in Apple Pay. Other types of biometrics are slowly emerging, including tools like Quixter, which uses handprint scans to authorize payments.[88] These tools will continue to be developed, though Discover predicts it will be 3-5 years before they really take off as the EMV migration to chip & PIN has tied the hands of merchants and Issuers alike.[89]

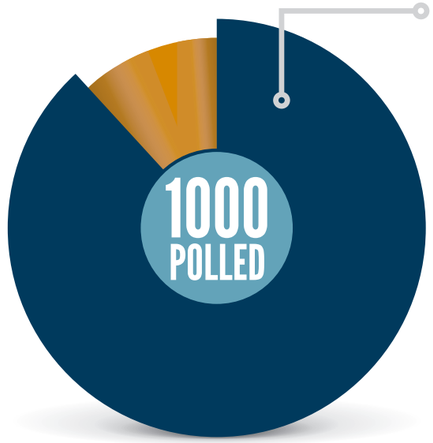
Existing and emerging payments companies are taking advantage of the blurring lines of card-present and card-not-present commerce. Companies like PayPal and Square are attempting to bridge the two worlds by integrating their mobile registers with consumer-facing device apps that also offer value-added services in an attempt to drive loyalty and collect additional consumer data.[90]

According to Javelin Strategy & Research, alternative payments are gaining traction as a percentage of overall online retail payments:[91]



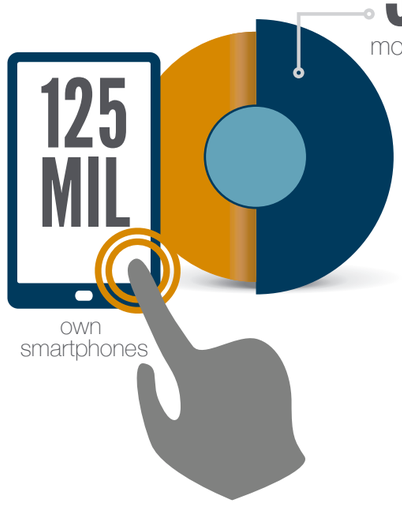
Mobile Snapshot

The global market for mobile wallet technology is projected to grow at a 36.8% CAGR over the next 4 years.[92] New mobile wallets continue to emerge globally, proliferated by the popularity and success of Apple Pay and Google Wallet. The inherent security of mobile wallets, which implement biometrics and tokenization, make them appealing to consumers. Additionally, merchants who are NFC-compatible stand to benefit in the loyalty department, if they can successfully weave mobile wallets into a loyalty program that extends beyond point rewards. Mobile and loyalty are intriguing to merchants because they offer new opportunities for partnerships and the ability to market to new customers, opening up incremental revenue streams when executed well.[93]

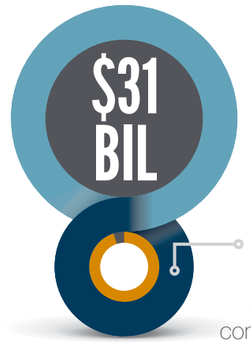


83%

Executives believe mobile payments will achieve widespread mainstream consumer adoption by the end of 2015



54%
mobile phone market



7%
electronic commerce sales

MOBILE WALLETS & THE NEED FOR AGILITY

One of the biggest hurdles the technology faces in adoption is establishing itself as a secure option. Given the data breaches over the past years, consumers are still highly sensitive about whose hands their data is in. Consumers today are savvier with how and where they put their personal information online and how that data is accessed, but are still generally wary about pushing any personal data into the digital realm. Lack of awareness about how mobile wallets use personal information as well as the security features used to protect data, consumer concerns about privacy and data can hinder mobile wallet adoption. Security and privacy issues must be thoroughly ironed out before adoption will largely take off.

In order to be sustainable, the integration of mobile and loyalty must be agile enough to add capabilities as the market grows to aid in retention. This type of comprehensive, adaptive mobile payments infrastructure is key. As the marketplace evolves and payments systems become more advanced, the infrastructure must enable merchants to do more than just process a transaction. The inertia of adopting a new payment method will require mobile payments to provide additional value.[94] When it comes to the intersection of mobile wallets and the new world of mobile loyalty, merchants need a gateway that is equipped to manage today's challenges and is agile enough to adapt to emerging technologies and demands of tomorrow.

Looking Ahead: Internet of Things

Technology is increasingly infiltrating all aspects of everyday life and payments is no exception. The Internet of Things (IoT) expands daily and as mobile payments and the proliferation of smartphone use continue, mobile payment capabilities will be facilitated through IoT. Companies have already begun developing digital signage, kiosks and intelligent vending machines, making payments possible through common things.[95] Mobile payment acceptance will merge with point-of-sale technology to enable consumers to shop through a variety of physical objects securely and will enhance how retailers can market and sell both remotely and in-store.

Gartner expects the Internet of Things installed base will grow by 2020 to include 26 billion units, generating $1.9 trillion.[96] To garner mainstream success will require partnerships across the value chain, a reasonable method of integration, and most importantly – security. By securing transaction data with tokenization, encryption, POS device management and other tools, merchants can engage consumers who feel comfortable and safe making payments through everyday things.

There are far-reaching implications to the payments industry, including the advancement of non-cash payments as well as greater access to data. An increased number of payment endpoints means huge potential gains for merchants with contactless payment technology enabled.[97] According to Bloomberg, this will largely contribute to the mobile transaction market, propelling payments to $90 billion in 2017, a 700% increase over 2012.[98]

The industry will widen as service providers aim to make every physical object a potential – and secure – place for commerce. Traditional bill pay will expand as consumers can control and pay for utilities and other things remotely via devices with embedded chips that carry the cardholders payment card information. Subscription and recurring business will see a shift too as consumer data helps shape new payment and billing models – businesses like gyms can update pricing models based upon customer usage, which can be tracked through wearables or even wireless sensor networks.[99]

For merchants, this highlights the importance of an agile payment processing operation. Merchants need an efficient, streamlined way to manage end-to-end chargeback, fraud and security protection. A processing gateway should provide deep insights from real-time analytics, optimize billings to improve customer loyalty and lower attrition. It is more critical than ever to have an adaptive gateway with the capacity to handle all aspects of payment processing in today's climate and that can manage the challenges – and maximize the opportunities – tomorrow will bring.

Conclusion

2014 was a turbulent year for payments and 2015 is shaping up to be equally erratic. EMV will be a game-changer for payments in terms of security, fraud costs and impacts to CNP commerce. As merchants tread the murky payments water into the uncertainty of tomorrow, these market forces paired with innovative technology will open up new opportunities and challenges for merchants. As the evolution of the payments ecosystem continues, the overall payment process will require a streamlined and compliant foundation supported by industry best practices. CNP merchants must continue to effectively address obstacles and maintain pace with current and emerging solutions to optimize payment processing and authorization.

Whether managed entirely in-house or via third-party, instituting sound practices in the payment processing life cycle contributes to process optimization, risk mitigation and increased profits. Subsequently, CNP merchants can see improvements in other key success metrics, including customer satisfaction, cost minimizations and the overall streamlining of business processes. CNP merchants that enact a proactive payment processing strategy instead of a reactionary one will find the payment ecosystem course easier to navigate and more apt to experience long-term business success.

About Verifi

Verifi™ is a premier provider of global electronic payment and risk management solutions. Since 2005, Verifi's best-in-breed offerings have helped card-not-present (CNP) merchants reduce risk while increasing profitability. The highly customizable payment and real-time reporting platform serves as a foundation for Verifi's suite of fraud solutions and risk management strategies. Our multi-layered approach enables transaction risk management and mitigation, billing optimization strategies, and total chargeback prevention and recovery services. Verifi is PCI Level 1 certified and headquartered in Los Angeles, California.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST
Main Fax: (323) 655-5537
Email Address: info@verifi.com
Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 No Author Listed. “Merchant Category Codes for IRS Form 1099-MISC Reporting”; visa.com; No Date Listed; http://web.archive.org/web/20070710202209/http://usa.visa.com/download/corporate/resources/mcc_booklet.pdf

2 No Author Listed. “Tips On How To Lower Your Credit Card Processing Costs and Fees”; Intuit.com, No Date Listed, http://payments.intuit.com/resources/reduce-credit-card-processing-costs.jsp

3 No Author Listed. “Tips On How To Lower Your Credit Card Processing Costs and Fees”; Intuit.com, No Date Listed, http://payments.intuit.com/resources/reduce-credit-card-processing-costs.jsp

4 McCabe, Laurie; “What Are Integrated Payment Solutions and Why Should You Care”; smallbusinesscomputing.com; January 31 2011; http://www.smallbusinesscomputing.com/biztools/article.php/3922966/What-Are-Integrated-Payment-Solutions-and-Why-Should-You-Care.htm

5 No Author Listed. “Tips On How To Lower Your Credit Card Processing Costs and Fees”; Intuit.com, No Date Listed, http://payments.intuit.com/resources/reduce-credit-card-processing-costs.jsp

6 Dwyer, Katherine; “Merchant Fees for Credit Card and Debit Card Transactions”; ct.gov; January 7 2013; http://www.cga.ct.gov/2013/rpt/2013-R-0015.htm

7 Matt Niehaus. “Making “Cents” of Credit Card Processing Fees”; instoredoes.com, August 28, 2013 https://instoredoes.com/blog/making-cents-of-credit-card-processing-fees

8 No author listed. “Payment Facilitators”; vantiv.com, no date listed. http://www.vantiv.com/Partner-with-us/Payment-Facilitators

9 No author listed. “Payment Service Provider”; wikipedia.org, last modified April 23, 2015. http://en.wikipedia.org/wiki/Payment_service_provider

10 No author listed. “IPSP & 3rd Party Processing Solutions”; onlineips.net, no date listed. http://www.onlineips.net/solutions/ipsp-3rd-party-processing-solutions/

11 No author listed. “IPSP & 3rd Party Processing Solutions”; onlineips.net, no date listed. http://www.onlineips.net/solutions/ipsp-3rd-party-processing-solutions/

12 Presented by the mobile payments committee of the electronic transactions association. “White Paper - beyond the hype: mobile payments for merchants”; 2013 http://www.electran.org/wp-content/uploads/FINAL-MPC-Merchant-White-Paper-3-11-13.pdf

13 No author listed. “Person-to-Person (P2P) Payments Online: What to Know Before You Click and Send That Money”; fdic.gov, Spring 2014 https://www.fdic.gov/consumers/consumer/news/cnspr14/p2p.html

14 Constine, Josh. “Facebook Introduces Free Friend-To-Friend Payments Through Messages”. Techcrunch.com; March 2015. http://techcrunch.com/2015/03/17/facebook-pay/#.b6dccb:uMPM

15 Constine, Josh. “Facebook Introduces Free Friend-To-Friend Payments Through Messages”. Techcrunch.com; March 2015. http://techcrunch.com/2015/03/17/facebook-pay/#.b6dccb:uMPM

16 Constine, Josh. “Facebook Introduces Free Friend-To-Friend Payments Through Messages”. Techcrunch.com; March 2015. http://techcrunch.com/2015/03/17/facebook-pay/#.b6dccb:uMPM

17 Constine, Josh. “Facebook Introduces Free Friend-To-Friend Payments Through Messages”. Techcrunch.com; March 2015. http://techcrunch.com/2015/03/17/facebook-pay/#.b6dccb:uMPM

18 Smith, Gordon; “Understanding Real-Time Payment Processing”. digitaltransactions.net; No Date Listed; www.digitaltransactions.net/public/frontend/files/1007networks2.doc

19 Smith, Gordon; “Understanding Real-Time Payment Processing”. digitaltransactions.net; No Date Listed; www.digitaltransactions.net/public/frontend/files/1007networks2.doc

20 Walker, Michael. “Batch vs. Real Time Data Processing”. datasciencecentral.com; August 2013. http://www.datasciencecentral.com/profiles/blogs/batch-vs-real-time-data-processing

21 Walker, Michael. “Batch vs. Real Time Data Processing”. datasciencecentral.com; August 2013. http://www.datasciencecentral.com/profiles/blogs/batch-vs-real-time-data-processing

22 Pritchard, Justin; “ACH Processing Basics”. banking.about.com; No Date Listed; http://banking.about.com/od/businessbanking/a/achprocessing.htm

23 No author listed. “Electronic Check Basics: What you need to know about eChecks or electronic checks”; quickbooks.intuit.com, no date listed http://quickbooks.intuit.com/facts-about-electronic-checks/

24 Adyen; “Optimizing payments to increase revenues: 8 Best Practices to enhance consumer experience and payment processing”. adyen.com; No Date Listed; https://www.adyen.com/dam/documentation/whitepapers/Adyen-Edgar-Dunn-Company-Report-Optimizing-Payments.pdf

25 Katey Troutman. “How Much Money Does a Data Breach Cost?”; cheatsheet.com, May 10, 2015 http://www.cheatsheet.com/business/how-much-does-a-data-breach-actually-cost.html/?a=viewall

26 No Author Listed. “Tokenization”. wikipedia.org; No Date Listed; https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

27 No Author Listed. “Tokenization”. wikipedia.org; No Date Listed; https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

28 No Author Listed. “EMVCo to Work on Payment Tokenization Standards”. Paymentsnews.com; January 2014. http://www.paymentsnews.com/2014/01/emvco-to-work-on-payment-tokenization-standards.html

29 No Author Listed. “EMVCo to Work on Payment Tokenization Standards”. Paymentsnews.com; January 2014. http://www.paymentsnews.com/2014/01/emvco-to-work-on-payment-tokenization-standards.html

30 No Author Listed. “EMVCo to Work on Payment Tokenization Standards”. Paymentsnews.com; January 2014. http://www.paymentsnews.com/2014/01/emvco-to-work-on-payment-tokenization-standards.html

31 Sarah Clark. “EMVCo publishes tokenization framework specification”; nfcworld.com, March 11, 2014 http://www.nfcworld.com/2014/03/11/328236/emvco-publishes-tokenization-framework-specification/

32 Sarah Clark. “EMVCo publishes tokenization framework specification”; nfcworld.com, March 11, 2014 http://www.nfcworld.com/2014/03/11/328236/emvco-publishes-tokenization-framework-specification/

33 EPX; “E2E Encryption + Tokenization Technology”. epx.com; No Date Listed; http://epx.com/epx-e2e-tokenization-technology/

34 Robin Arnfield. “Loyalty schemes will drive mobile wallet adoption”; mobilepaymentstoday.com, March 28, 2014 http://www.mobilepaymentstoday.com/articles/loyalty-schemes-will-drive-mobile-wallet-adoption/

35 Robin Arnfield. “Loyalty schemes will drive mobile wallet adoption”; mobilepaymentstoday.com, March 28, 2014
http://www.mobilepaymentstoday.com/articles/loyalty-schemes-will-drive-mobile-wallet-adoption/

36 Christine Kern. “Retail Breaches Alter Customer Attitudes and Behavior”; retailsolutionsonline.com. July 10, 2014
http://www.retailsolutionsonline.com/doc/retail-breaches-alter-customer-attitudes-and-behavior-0001

37 The Chartered Institute of Marketing. “Cost of customer acquistion vs customer retention”; camfoundation.com, 2010
http://www.camfoundation.com/PDF/Cost-of-customer-acquisition-vs-customer-retention.pdf

38 No Author Listed; “PCI Security Standards For Merchants; pcisecuritystandards.org; No Date Listed;
https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

39 PCI Security Standards Council. “Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard”;
pcisecuritystandards.org, August 2013, https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

40 EPX; “E2E Encryption + Tokenization Technology”. epx.com; No Date Listed; http://epx.com/epx-e2e-tokenization-technology/

41 PCI Compliance Guide; “PCI FAQS”. pcicompliance.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#5

42 American Express; “The Data Security Operating Policy”. americanexpress.com; No Date Listed;
https://www209.americanexpress.com/merchant/services/en_US/data-security

43 No Author Listed; “PCI Compliance: Basics for Credit Card Security”; braintreepayments.com; No Date Listed;
https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security

44 Ed Moyle. “PCI DSS version 3.0: The five most important changes for merchants”; searchsecurity.techtarget.com, no date listed
http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

45 Ed Moyle. “PCI DSS version 3.0: The five most important changes for merchants”; searchsecurity.techtarget.com, no date listed
http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

46 Ed Moyle. “PCI DSS version 3.0: The five most important changes for merchants”; searchsecurity.techtarget.com, no date listed.
http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

47 Ed Moyle. “PCI DSS version 3.0: The five most important changes for merchants”; searchsecurity.techtarget.com, no date listed
http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

48 Ed Moyle. “PCI DSS version 3.0: The five most important changes for merchants”; searchsecurity.techtarget.com, no date listed
http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

49 No Author Listed; “PCI FAQs”; pcicomplianceguide.org; No Date Listed; http://www.pcicomplianceguide.org/pcifaqs.php#11

50 No Author Listed; “PCI Noncompliant Consequences”; focusonpci.com; No Date Listed;
http://www.focusonpci.com/site/index.php/PCI-101/pci-noncompliant-consequences.html

51 Adam Woozeer. “PCI DSS compliance and minimizing your costs”; cognia.com, July 16,2014
http://www.cognia.com/blog/pci-dss-compliance-minimizing-costs/

52 No Author Listed. “The Impacts of EMV”; verifi.com, 2014. http://verifi.com/wp-content/uploads/2014/11/Verifi_wp_Impact-EMV.pdf

53 No Author Listed. “Understanding the 2015 U.S. Fraud Liability Shifts”. emv-connection.com; May 2015.
http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf

54 Dick Mitchell. “Missing the EMV Liability Shift Bears a Huge Cost”; paymentssource.com, August 4, 2014
http://www.paymentssource.com/news/paythink/missing-the-emv-liability-shift-bears-a-huge-cost-3018661-1.html

55 No Author Listed. “EMVCo to improve standard for e- and m-commerce”. Greensheet.com; January 2015.
http://www.greensheet.com/emagazine.php?story_id=4263

56 No Author Listed. “2014 Fraud Spike Cost US Retailers $32 Billion”; pymnts.com, February 17, 2015
http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/#.VUzj60tkf8E

57 No Author Listed. “Annual Report: 2014 LexisNexis® True Cost of Fraud℠ Study”; lexisnexis.com, August 2014
http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

58 No Author Listed. “Annual Report: 2014 LexisNexis® True Cost of mCommerce”; lexisnexis.com,January 2015
http://lexisnexis.com/risk/downloads/whitepaper/true-cost-fraud-mobile-2014.pdf

59 No Author Listed. “75 million new malware strains recorded in 2014: Report”; businessinsurance.com, No date.
http://www.businessinsurance.com/article/20150305/NEWS09/150309912/75-million-new-malware-strains-recorded-in-2014-report

60 No Author Listed. “Will The Liability Move Most US Merchants To EMV?”; pymnts.com, January 22, 2015
http://www.pymnts.com/news/2015/will-the-liability-move-most-u-s-merchants-to-emv/#.VVHyaEtkf8E

61 Ori Bach. “Combatting Account Takeover Fraud & Remote Access Trojans”; bankinfosecurity.com, No date.
http://www.bankinfosecurity.com/webinars/chasing-down-rats-combatting-account-takeover-fraud-at-age-remote-w-646

62 No Author Listed. “75 million new malware strains recorded in 2014: Report”; businessinsurance.com, No date.
http://www.businessinsurance.com/article/20150305/NEWS09/150309912/1245

63 Mohit Kumer. “Rombertik Malware Destroys Hard Drives to Avoid Dection”; thehacknews.com, May 5, 2015
http://thehackernews.com/2015/05/malware-destroy-hard-drive.html

64 Nicholls, Charles. “Are Verified by Visa and MasterCard SecureCode Conversion Killers?”; practicalecommerce.com; June 14 2013;
http://www.practicalecommerce.com/articles/4059-Are-Verified-by-Visa-and-MasterCard-SecureCode-Conversion-Killers-.

65 Finsphere; “Five Words Nobody Likes To Hear: Your Credit Card Was Declined”. finsphere.com; April 19 2013;
http://blog.finsphere.com/2013/04/19/five-words-nobody-likes-to-hear-your-credit-card-was-declined/

66 Al Pascual. “The Consumer Data Insecurity Report: Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas”;
javelinstrategy.com, No date. https://www.javelinstrategy.com/uploads/web_brochure/TheConsumerDataInsecurityReport_byNCL.pdf

67 Al Pascual. “The Consumer Data Insecurity Report: Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas”;
javelinstrategy.com, No date. https://www.javelinstrategy.com/uploads/web_brochure/TheConsumerDataInsecurityReport_byNCL.pdf

68 Al Pascual. “The Consumer Data Insecurity Report: Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas”;
javelinstrategy.com, No date. https://www.javelinstrategy.com/uploads/web_brochure/TheConsumerDataInsecurityReport_byNCL.pdf

69 Al Pascual. “The Consumer Data Insecurity Report: Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas”;
javelinstrategy.com, No date. https://www.javelinstrategy.com/uploads/web_brochure/TheConsumerDataInsecurityReport_byNCL.pdf

70 TJ Horan. “Improved Analytics Can Boost the Fraud Fight”; paymentssource.com, Mayb5, 2014
http://www.paymentssource.com/news/paythink/improved-analytics-can-boost-the-fraud-fight-3017781-1.html

71 TJ Horan. “Improved Analytics Can Boost the Fraud Fight”; paymentssource.com, Mayb5, 2014
http://www.paymentssource.com/news/paythink/improved-analytics-can-boost-the-fraud-fight-3017781-1.html

72 Ashley Poynter. Balancing Omni-Channel Opportunity with Increased Risk"; verifi.com, No date.
http://www.verifi.com/in-the-news/balancing-omni-channel-opportunity-with-increased-risk/

73 Ashley Poynter. Balancing Omni-Channel Opportunity with Increased Risk"; verifi.com, No date.
http://www.verifi.com/in-the-news/balancing-omni-channel-opportunity-with-increased-risk/

74 No Author Listed. "Annual Report: 2014 LexisNexis® True Cost of Fraud℠ Study"; lexisnexis.com, August 2014
http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

75 No Author Listed. "Credit Card Payments: Chargebacks & Fraud Liability"; fraudpractice.com, No date. http://www.fraudpractice.com/fl-paychargeback.html

76 LexisNexis; "True Cost of Fraud Study"; lexisnexis.com; 2013; http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

77 Dalpay; "Understanding Chargebacks". dalpay.com; No Date Listed; https://www.dalpay.com/en/support/chargebacks.html

78 No Author Listed; "Friendly Fraud"; Wikipedia.org; No Date Listed; http://en.wikipedia.org/wiki/Friendly_fraud

79 Harper, Elizabeth; "Friendly fraud? Yes it exists". csmonitor.com; March 11, 2014;
http://www.csmonitor.com/Business/Saving-Money/2014/0311/Friendly-fraud-Yes-it-exists

80 No Author Listed; "Chargeback Cycle"; visa.com; No Date Listed;
https://usa.visa.com/merchants/merchant-support/dispute-resolution/chargeback-cycle.jsp

81 No Author Listed. "Telecommunication Industry: Global Fraud Prevention and Best Practices for Visa Merchants"; visa.ca; No Date Listed;
http://www.VISA.ca/merchant/resources/fraud-fighting/pdf/telecommunication-industry-global-Fraud-Prevention.pdf

82 No Author Listed. "Telecommunication Industry: Global Fraud Prevention and Best Practices for Visa Merchants"; visa.ca; No Date Listed;
http://www.VISA.ca/merchant/resources/fraud-fighting/pdf/telecommunication-industry-global-Fraud-Prevention.pdf

83 Sumit Sood and Joseph Pinipe. "Card Disputes and Chargebacks"; wipro.com, January 2014
http://www.wipro.com/documents/card-disputes-and-chargebacks.pdf

84 No Author, Liste. "Issuer Alerts Technique Overview"; fraudpractice.com, No date. http://www.fraudpractice.com/FL-Issuer-Alerts.html

85 Elizabeth Palermo. "10 Worst Data Breaches of All Time"; tomsguide.com , February 6, 2015
http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html

86 Jao, Jerry; "Customer Retention Should Outweigh Customer Acquisition". cmo.com; August 2 2013;
http://www.cmo.com/articles/2013/7/18/customer_retention.html

87 Mastercard Automatic Billing Updater, http://www.mastercard.com/us/wce/PDF/Billing%20Updater%20Brochure_10%2006.pdf, p.4.,
According to Mastercard Authorization Data

88 No Author Listed. "11 Noteworthy Uses of Biometrics in Payments"; paymentssource.com , No date.
http://www.paymentssource.com/gallery/11-noteworthy-uses-of-biometrics-in-payments-3017619-1.html

89 No Author Listed. "11 Noteworthy Uses of Biometrics in Payments"; paymentssource.com , No date.
http://www.paymentssource.com/gallery/11-noteworthy-uses-of-biometrics-in-payments-3017619-1.html

90 John Heggestuen. "Emerging Payment Technologies Will Create New Winners And Losers In The Giant Credit Card Industry";
businessinsider.com, September 18, 2014. http://www.businessinsider.com/new-credit-card-industry-market-competition-2014-5

91 Daly, Jim "Report Documents the March of Online Alternatives to the Payments Mainstream"; digitaltransactions.net; March 9 2014;
http://www.digitaltransactions.net/news/story/4556

92 Jes Ellacott. "Mobile Wallet Still Struggling to Capture Consumers, Despite Projected Growth"; technavio.com, March 10, 2015
http://www.technavio.com/blog/mobile-wallet-still-struggling-to-capture-consumers-despite-projected-growth

93 Steven Norton. "The Next Step for the Mobile Wallet? Loyalty Programs"; http://blogs.wsj.com, Jan 26, 2015
http://blogs.wsj.com/cio/2015/01/26/the-next-step-for-the-mobile-wallet-loyalty-programs/

94 No Author Listed. "The Mobile Wallet: How Loyalty Could Spur Consumer Adoption of Mobile Payments"; euromonitor.com, No date.
http://www.euromonitor.com/the-mobile-wallet-how-loyalty-could-spur-consumer-adoption-of-mobile-payments/report

95 No Author Listed. "Intel Pushes Payments Into The Internet Of Things"; pymnts.com, April 6th, 2015
http://www.pymnts.com/news/2015/ingenico-and-intel-tie-up-for-payments-on-the-internet-of-things/#.VUtjp0tkf8E

96 No Author Listed. "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 "; gartner.com, December 12, 2013
http://www.gartner.com/newsroom/id/2636073

97 Hailey Winston. "The Internet of Things Will Revolutionize the Payment Industry"; yaleeconomicreview.org, November 11, 2014
http://www.yaleeconomicreview.org/archives/2204

98 Hailey Winston. "The Internet of Things Will Revolutionize the Payment Industry"; yaleeconomicreview.org, November 11, 2014
http://www.yaleeconomicreview.org/archives/2204

99 Hailey Winston. "The Internet of Things Will Revolutionize the Payment Industry"; yaleeconomicreview.org, November 11, 2014
http://www.yaleeconomicreview.org/archives/2204

For More Information

Main Phone: (323) 655-5789
Mon-Fri 8:00 AM – 5:00 PM PST

Main Fax: (323) 655-5537

Email Address: info@verifi.com

Mailing Address:
8391 Beverly Blvd.
Box #310
Los Angeles, CA 90048