Accepting Credit Card Payments

What Governments should know about Vendor Services, Fees, and Risks

May 13, 2021

Matthew P. Leman

Executive Director

J.P. Morgan

J.P.Morgan

Merchant Services US Disclaimer

This presentation was prepared exclusively for the benefit and internal use of the Chase client or potential Chase client to whom it is directly delivered and/or addressed (including subsidiaries and affiliates, the "Company") in order to assist the Company in evaluating, on a preliminary basis, the feasibility of a possible transaction or transactions or other business relationship and does not carry any right of publication or disclosure, in whole or in part, to any other party. This presentation is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by Chase. Neither this presentation nor any of its contents may be disclosed or used for any other purpose without the prior written consent of Chase. This presentation does not constitute a commitment by any Chase entity to extend or arrange credit or to provide any other services to Company.

In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. The statements, views, and opinions that will be expressed during the presentation are those of the presenters and are not endorsed by, or reflect the views or positions of, Chase. The information herein may not take into account individual client circumstances, objectives or needs and is not necessarily intended as a recommendation of a particular product or strategy to the Company and Company shall make its own independent decision. Chase is not liable for decisions made or actions taken in reliance on any of the information covered during the presentation. Furthermore, Chase makes no representations as to the actual value which may be received in connection with a transaction or use of the products and services mentioned nor the legal, tax or accounting effects of consummating a transaction.

Chase, Chase Paymentech, Chase Merchant Services, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "Chase") and if and as used herein may include as applicable employees or officers of any or all of such entities irrespective of the marketing name used. Products and services may be provided by commercial bank affiliates, securities affiliates or other Chase affiliates or entities. In particular, securities brokerage services other than those which can be provided by commercial bank affiliates under applicable law will be provided by registered broker/dealer affiliates such as J.P. Morgan Securities LLC, J.P. Morgan Institutional Investments Inc. or by such other affiliates as may be appropriate to provide such services under applicable law. Such securities are not deposits or other obligations of any such commercial bank, are not guaranteed by any such commercial bank and are not insured by the Federal Deposit Insurance Corporation. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by Chase or its affiliates/subsidiaries.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates

JPMorgan Chase and its affiliates do not provide tax, legal or accounting advice. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, tax, legal or accounting advice. You should consult your own tax, legal and accounting advisors before engaging in any transaction or if you have any questions. In addition, any discussion of U.S. tax matters included herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone not affiliated with Chase of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties.

J.P.Morgan

Agenda

		Page
1	**Fundamentals of credit card processing**	**1**
2	Risk management and data security	6
3	PCI compliance	18
4	Trends in payments	25

Elements of a card transaction

Whether at the point of sale, online or on a mobile device, the fundamental elements of a card transaction are the same.

Authorization

Confirms sufficient funds and renders the authorization amount unavailable for other purchases

Clearing and settlement

Clearing: Merchant sends purchase information to the network, which in turn sends to the issuing bank

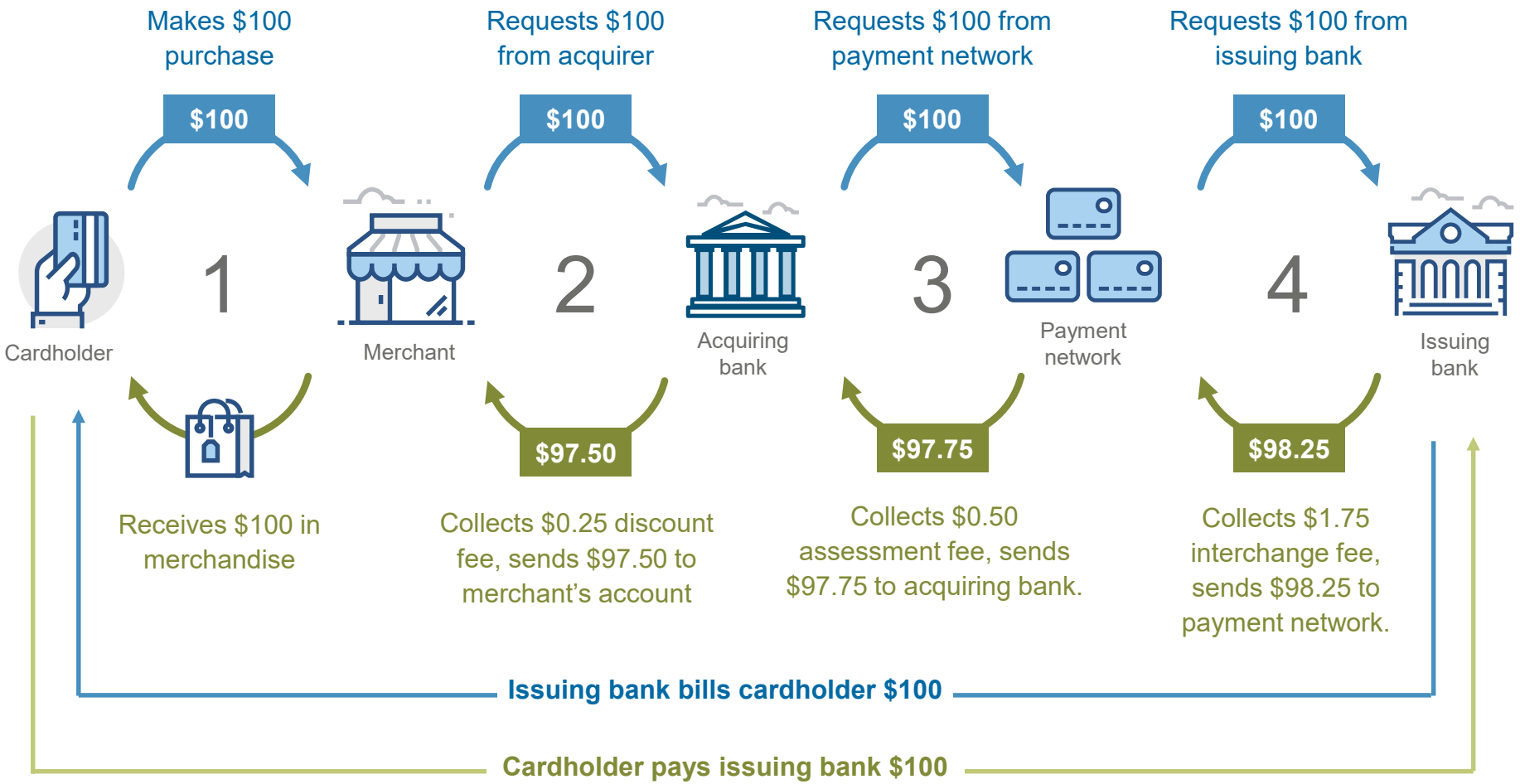
Settlement: issuing bank sends payment to the payment network, which in turns sends payment to the merchant acquirer

Funding

Acquirer (or payment network) pays the merchant for their activity

How does a payment work?

The traditional interchange and transaction flow



For illustrative purposes only, these are not JP Morgan prices

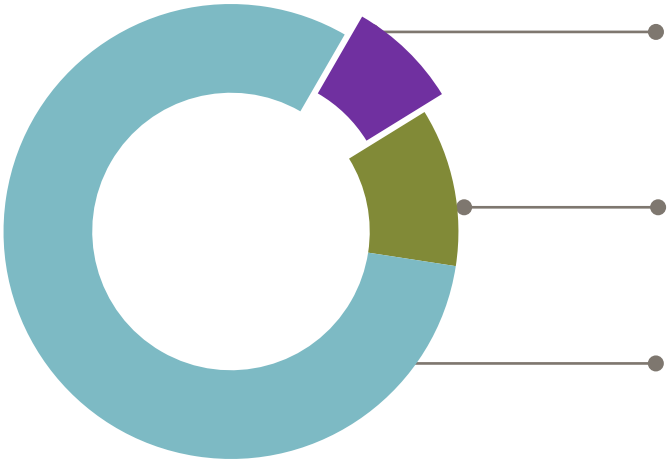
J.P.Morgan

What makes up a transaction fee?

Industry-wide model for payment processing

Transaction fees are broken down into three parts: Processor, network and interchange. Each of these fees represents a different service or risk associated with the transaction.

Transaction fee components



Processor fee

Assessed by a merchant services provider for coordinating authorization, settlement, chargebacks, reporting and customer service

Network fee (switch fee)

Assessed by payment networks for the use of their respective network

Interchange fee

Assessed by the payment networks to compensate issuers for the risk and cost of a card transaction

Polling Question #1

Make sure you qualify transactions for the best interchange rate

Control your processes to help manage costs

Interchange fees cover the cost of issuing cards and mitigating fraud claims

Set up by the payment networks, interchange:

- Creates incentives for payment network participants to maintain a reliable, dynamic and secure electronic commerce environment.
- Promotes card use.
- Encourages clients to process payments securely.
- Efficient and compensates issuers for the risk and cost of real-time transaction enablement.

Several factors that determine a transaction's interchange fee are under your control.

Within your control

- **Use the most secure authorization method**
  Insert chip or swipe magnetic strip – avoid manual key entry
- **Capture Level II and Level III data**
  Additional information helps to mitigate risk in the eyes of the payment brands

Outside of your control

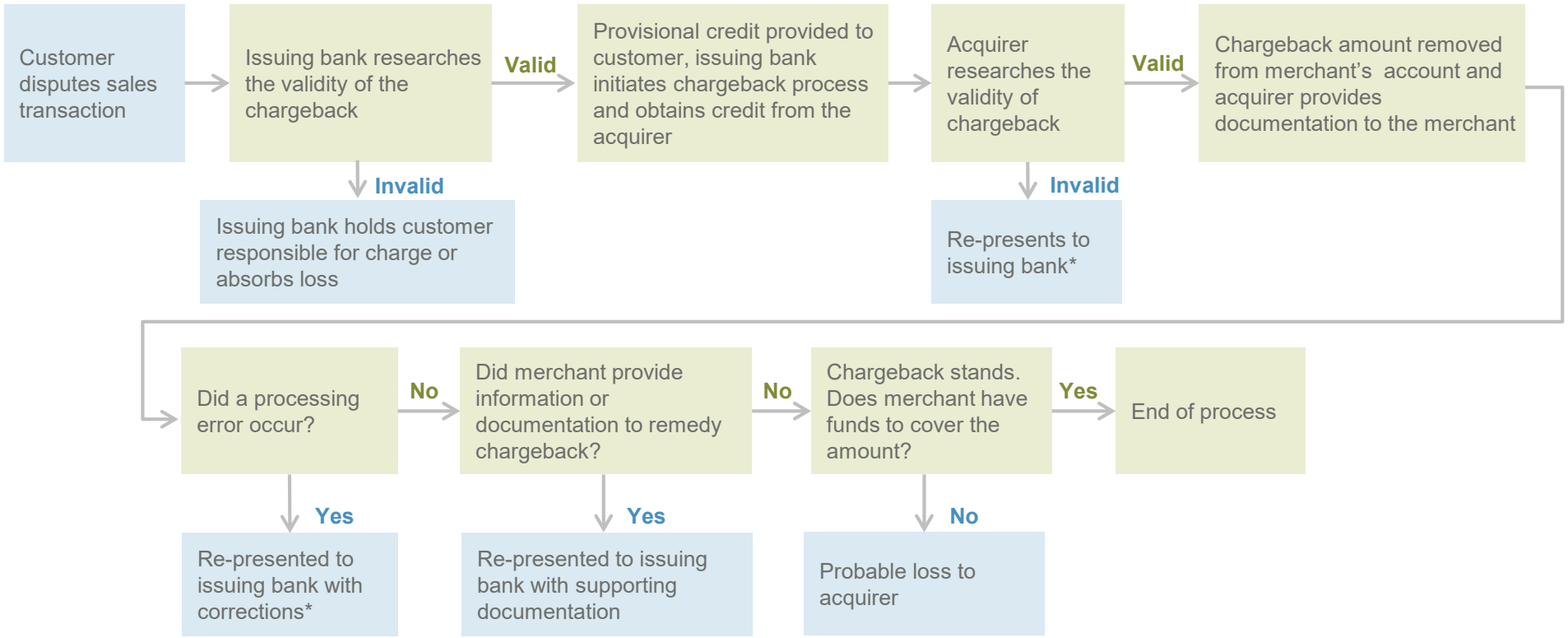
- **Type of card presented by consumer**
  Reward and commercial cards have higher interchange relative to general purpose cards
- **Transaction type**
  Card-not-present transactions have higher interchange relative to card-present transactions

Agenda

		Page
1	Fundamentals of credit card processing	1
2	**Risk management and data security**	**6**
3	PCI compliance	18
4	Trends in payments	25

How do chargebacks work?

A traditional chargeback process



*The payment brands act as a payment clearinghouse between the issuing bank and acquiring bank during the chargeback and re-presentment process. A compliance resolution process also exists at the bank card association if no chargeback rights are available to the issuing bank and a financial loss is incurred as a result of bank card association rules.

A second chargeback may occur if the re-presentment is invalid, documentation did not support the charge or another chargeback reason code applies. If the acquirer disputes the second chargeback presentment, the acquirer may file an appeal for arbitration with the bank card association. Re-presentment is not allowed for a second chargeback

Fraud protection helps merchants keep more of the revenue they earn

Protection from fraud protects revenue and reputation

Fraud is an expensive problem. Not only does increased fraud result in expensive chargebacks, it affects an organization's reputation too, resulting in increased costs due to lost revenue.

Your risks:

- **Stolen data** Individuals target merchants to steal customer card data to make more fraudulent purchases
- **Stolen data from another merchant** Company, employee, supplier and vendor data can be stolen from another merchant

Fraudsters attack using several methods:

- **Fraudulent cards** Fraudsters test stolen credit card numbers with small incremental purchases before making large ones
- **Man in the middle** A hacker intercepts and captures valuable data submitted to a site, such as payment information
- **Physical breach** Sensitive documents and files can be vulnerable to a theft or accidental exposure if not kept physically secured.

Protect your data at every step with a comprehensive approach to data security

Collect → Store → Transact

Collect

Card information is captured at point of sale and online.

Encryption
Protect primary account number (PAN) data in transit through your network and while it travels to Merchant Services from moment of capture at retail point-of-sale or from your website.

EMV
Help prevent skimming, counterfeit and lost/stolen fraud with advanced chip card technology.

Store

Card data is stored for future use.

Tokenization
Protect data while at rest by replacing payment data with a secure token that cannot be converted back to card or account information within your network.

Transact

Customer identity is authenticated and fraud risks managed.

Fraud tools
Provide greater visibility into sophisticated fraud patterns, which can help reduce fraud and manual review and pinpoint a transaction's origin in real time and dynamic order linking.

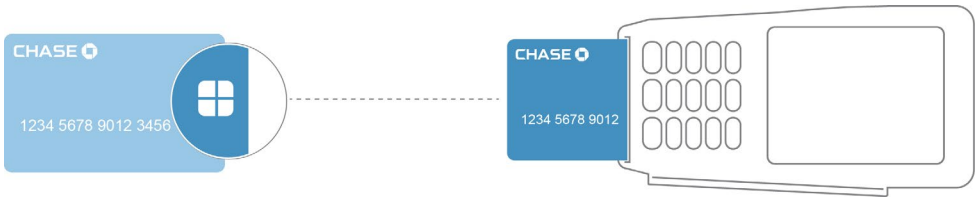
EMV
EMV utilizes dynamic data that help protect transactions.

Card-present
A type of transaction in which the card is physically swiped, tapped or dipped through a reader to capture details in person at point of sale.

Card-not-present
A type of card transaction in which the card is not present at the point of sale for the magnetic stripe to be read.

Added security with EMV card processing

EMV provides a secure method to exchange sensitive debit and credit card data between you and your payors.



How is this different from magstripe?

Magstripe
Data is the same from transaction to transaction.
(Valuable to fraudsters to make counterfeit cards)

Chip/EMV
Each transaction uses a unique transaction code that cannot be reused (Not valuable to fraudsters)

What are the benefits of accepting EMV?

- Shifts liability of fraud from you to the issuer
- Makes counterfeit nearly impossible since transaction codes can only be used once
- Fraudsters are targeting places using magnetic stripe terminals over EMV terminals

Fraud liability shift as of October 2015 (payment brand initiative to support EMV adoption)*

Liability for card-present fraud falls on the party that is the least secure EMV technology used in a fraudulent transactions.

Card type	*Terminal type*	*Liability*
Magstripe	Swipe	Issuer
Magstripe	Chip	Issuer
Chip	Chip	Issuer
Chip	Swipe	Merchant

Petro Automated Fuel Dispensers (AFD) (MCC 5542) liability shift:

October 2017 – Internationally issued chip cards used at non-EMV automated fuel dispensers (AFDs) in the U.S.

April 2021 - U.S. domestic-issued chip cards used at non-EMV AFDs in the U.S.

*The liability shift is required by the payment brands.

J.P.Morgan

Polling Question #2

How layered security protects transactions

EMV chip technology is only one component of an overall fraud and security strategy that card-present merchants must consider to protect themselves from rising fraud losses in the U.S. To fully protect your payment environment, you should consider coupling EMV with security solutions like encryption and tokenization.

	Card-present			Card-not-present		
Threats	EMV	Encryption	Tokenization	EMV	Encryption	Tokenization
Counterfeit cards	✓					
Lost and stolen cards	✓					
Reusing stolen data	✓*	✓	✓		✓	✓
Stealing data in transit		✓	✓		✓	✓
Stealing data at rest		✓	✓		✓	✓

- **EMV**: Card authentication, cardholder verification and dynamic data.
- **Encryption**: Point-to-point or end-to-end.
- **Tokenization**: Replaces card data with limited-use tokens.

Note: PCI-DSS compliance is still required with EMV.

*When used with PIN Cardholder Verification Method (CVM)

Protecting the card number from the moment of capture

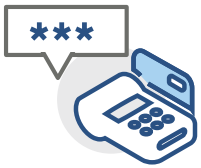
Encryption and Tokenization

Encryption solutions enable clients to protect primary account numbers (PAN). The data is captured and secured at your point of sale, and tokens are sent in the response messages to eliminate clear card data from your network.

The combination of encryption and tokenization can help protect your organization

- Helps eliminate the need to process, transmit and store unprotected account information on your systems
- May lower Payment Card Industry (PCI) requirements and compliance costs
- Potentially reduces risk if a system breach occurs, encrypted data is useless without decryption keys
- Easy integration available for terminals, or can be integrated with POS and enterprise applications

How these solutions work together



Customer's card data is **encrypted and formatted at the point of sale**.

An algorithm reformats the data so the POS system processes it in the same manner as previously unencrypted data.

Encrypted data is transmitted to your processor, **decrypted and processed through the payment brand networks**.

Your processor replies with a token for future use.

J.P.Morgan

What is tokenization?

Replacing real account data with a substitute value or token

Why is tokenization important?

Card data is valuable. Criminals can sell it for up to $20 per per card*. Tokenization makes high-value data almost useless.

- Data swiped from merchants using malware is sold in underground markets. Thieves use the data to commit fraud.
- Tokens were created to minimize risk for merchants who stored live payment account credentials on their servers.
- Network-wide tokens are being deployed to minimize risks throughout the ecosystem, including merchants, issuers, networks, acquirers and consumers.

Think of tokens like arcade tokens

Tokenization is like going to the cashier, giving cash and receiving tokens. Detokenization is like going back to the cashier and trading tokens for cash.

Tokens are lower risk

- Tokens are only valuable in limited context and for specific use, like playing games in an arcade.
- Criminals can't sell token data, which discourages them from attacking merchants.

How it works

Customer makes a credit card purchase. Data is **encrypted at the point of sale.**

Encrypted payment details are passed, and then **decrypted and processed through the payment networks**.

Your processor responds with a token. **The token is processed like a credit card payment.** Card data stays safe.

Source: Krebs On Security, E-Retail Hacks More Lucrative Than Ever, April 30, 2019

J.P.Morgan

Polling Question #3

Accept online payments securely and potentially reduce your PCI scope

Hosted Payment Solutions

Offer payors a seamless payment experience.

- Maintain total control of your payment page
- Control the branding (look and feel)
- Change payment page elements at any time

May reduce cost and scope of PCI compliance

View transactions, refunds and catalog payments

Safe and secure customer checkout

Minimize initial and ongoing IT expense

Customer experience

1. Payor decides to make purchase and heads to checkout.

2. Depending on the Hosted Payment Solution, the payor is either directed to another page or stays on the same one and enters their payment information

Your experience

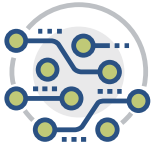
The transaction is sent to your processor to authenticate and process, sending approval to merchant website and confirmation to cardholder.

Card-not-present: Real-time fraud management with our robust fraud detection solution

Fraud Tools

Manage fraud in real-time with multidimensional screening technology

- **Multilayer device fingerprinting –** Assigns an ID number to the device that is being used to make a purchase.
- **Proxy piercing –** Provides geographic location and type of network the transaction is being made on.
- **Third-party identity verification –** You may choose to gather information from other verification services



Find hidden insights with advanced AI machine learning technology

- **Dynamic order linking –** Analyzes common characteristics across multiple purchases from yours and other businesses while transactions are occurring.
- **Continuous transaction monitoring –** Analyzes transactions during and after authorization for up to two weeks, giving you a chance to cancel the order before shipment.
- **Artificial intelligence:** Unsupervised and supervised machine learning using hundreds of data points

Best practices and fraud expertise using human intelligence

- **Enterprise workflow management –** Automatically have your transactions reviewed and immediately make a decision about whether or not the transaction should be authorized.
- **Custom rules management –** Customize rules in real time to determine types of transactions to review.
- **Business intelligence reporting –** Real-time reporting containing hundreds of variables to identify what transactions may be real or fraudulent

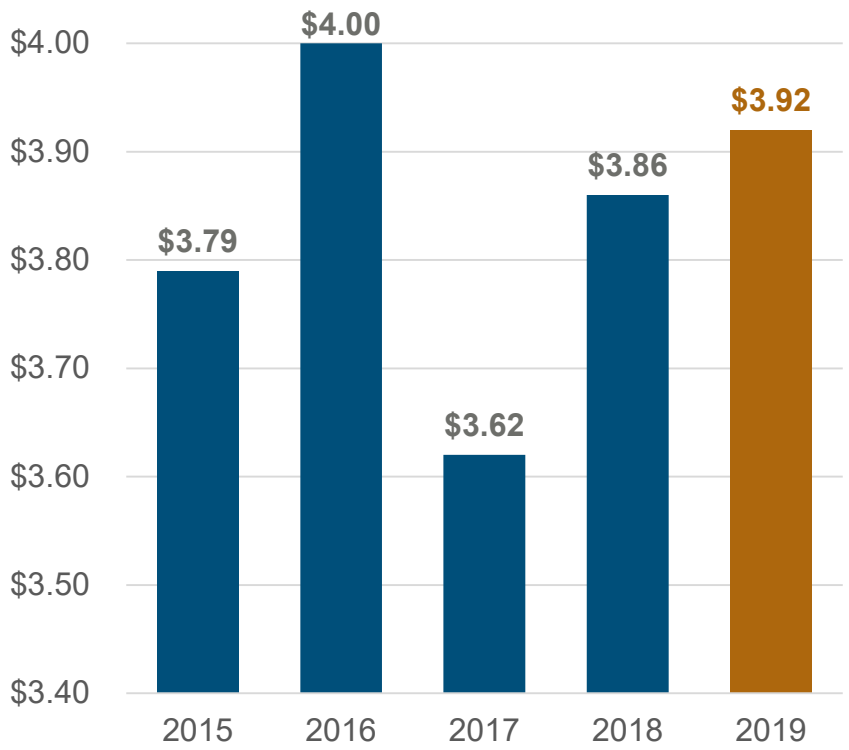
Polling Question #4

Agenda

		Page
1	Fundamentals of credit card processing	1
2	Risk management and data security	6
3	**PCI compliance**	**18**
4	Trends in payments	25

Data breaches continue to be costly for organizations

The global average total cost of a data breach (USD millions)



Key considerations in evaluating your security needs

- Data breaches are the most costly in the U.S., with a total average cost at $8.19 million in 2019
- The faster a data breach can be identified and contained, the lower the costs
- Companies that identified a breach in less than 100 days saved more than $1 million
- The average time to identify and contain a breach has increased since 2018; with average time in 2019 being 206 days and 73 days, respectively
- 51% of all breaches in 2019 were caused by malicious cyber attacks
- The loss of customer trust has serious financial consequences; The average cost of lost business for organizations in 2019 was $1.42 million

Source: Ponemon Institute (sponsored by IBM Security), 2019 Cost of a Data Breach Study: Global Overview, June 2019

What is the Payment Card Industry Data Security Standard?

A combined focus on process, people and technology

The Payment Card Industry Data Security Standard (PCI DSS) represents a combination of preventative, detective and responsive controls applied to a merchant's process, people and technologies. PCI DSS is not a one-time event; it is an active effort that involves constant monitoring and updates as threats and attacks evolve.

PCI DSS involves the management of all risk associated with card data in a business–from access to data at rest, to card skimming at the point of sale, to customer and employee shrinkage.

Keys to PCI DSS success

Process	People	Technology
Rationalize acceptance processes to reduce storage processing and transmission of cardholder data	Provide ongoing training for handling payment cards	PIN transaction security (PTS)-validated terminals protect against tampering and skimming
Security policies and procedures that comply with PCI DSS	Implement organization-wide security policy	Payment application DSS validation ensures PCI-grade security is built into the POS system
Consistent processes and routines to protect card data and remain PCI DSS compliant	Adopt best practice security procedures	Point-to-point encryption and tokenization technologies further reduce scope and risk

Check out the PCI Security Standards Quick Reference Guide for more information.

J.P.Morgan

Payment Card Industry Data Security Standard compliance overview

Goals	PCI DSS requirements
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 cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 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 network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors

PCI Data Security Standard (PCI DSS)

Your PCI level and validation requirements

Visa / Mastercard merchant levels		Validation actions	
Merchant level criteria	PCI security assessment type	PCI security assessment doc	Network vulnerability scans (ASV scans)
Level 1: 6+ million transactions annually from any acceptance channel with one card brand	On-site assessment with a Report on Compliance	ROC and AOC submitted to acquirer annually (QSA or ISA required)	Required quarterly
Level 2: 1-6 million transactions annually from any acceptance channel with one card brand	On-site assessment with a Report on Compliance or Self Assessment questionnaire	SAQ and AOC submitted to acquirer annually (QSA or ISA required)	Required quarterly – depending on questionnaire used
Level 3: 20,000 to 1 million e-commerce transactions annually with one card brand	Self Assessment Questionnaire	SAQ and AOC submitted to acquirer annually	Required quarterly – depending on questionnaire used
Level 4: Less than 20,000 e-commerce or less than 1 million transactions from any acceptance channel annually with one card brand	Self Assessment Questionnaire	SAQ and AOC required annually (submission to acquirer not mandatory)	Required quarterly (submission to acquirer not mandatory)

Fines for Non-compliance

Visa
- Level 1 - $10,000 monthly
- Level 2 - $5,000 monthly

Mastercard.
- Levels 1 & 2 - $25,000 for the first violation; doubles every quarter up to $200,000
- Level 3 - $10,000 for the first violation; doubles every quarter up to $80,000

Key considerations

- Risk of fines for non-compliance

Current and future-state features

Both non-validated and validated point-to-point encryption may help reduce your PCI scope

Non-validated point-to-point encryption (P2PE)

- Credit card number is encrypted when swiped, dipped, contactless or manually entered.
- Clear card is never in the merchant environment.
- The card number is encrypted at the merchant and is not unencrypted until it enters the secure environment of the acquirer.
- Leverages industry standards for encryption practices.

Validated point-to-point encryption (P2PE)

- P2PE adds processes to monitor encrypted transactions, alert merchants when problems occur and track devices throughout their lifecycle. A validated P2PE solution will be listed on the PCI website.
- Credit card number is encrypted when swiped, dipped, contactless or manually entered.
- Clear card is never in the merchant environment.
- The card number is encrypted at the merchant and is not unencrypted until it enters the secure environment of the acquirer, gateway or VAR.
- Triple DES DUKPUT is the most secure industry encryption standard used for protecting credit transactions.

Additional processes required for validated P2PE solutions

P2PE adds additional processes for the management of terminals and the monitoring of encrypted transactions:

- **Monitoring:** The system monitors every transaction to make sure the transaction is being processed by an approved device and that the terminal is encrypting the transaction correctly.
- **Alerting:** The system immediately alerts the merchant if there is an abnormality in the encryption environment.
- **Terminal tracking:** The system documents the tracking of a terminal from the point where the encryption key is injected, to the point the tamper-proof packaging is opened and documents the location of the device while in use.

Things to consider with PCI DSS

Required for any organization that accepts card payments

The PCI security standards council was created to help us understand and implement security, technology standards to protect our payment systems from breaches

Highlights	Things to consider
PCI compliance is not a one-time event	Ongoing effort that involves constant monitoring as threats and attacks evolve
Organizations that accept cards can be significantly impacted by PCI	PCI-enabled security technology can help minimize your PCI DSS scope
Noncompliance risk	Penalties can range from $5,000 to $500,000
Focus on the long term	Be proactive instead of reactive
Liability	In addition to financial, there is brand image and consumer confidence risk

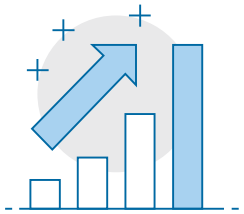
J.P.Morgan

Polling Question #5

Agenda

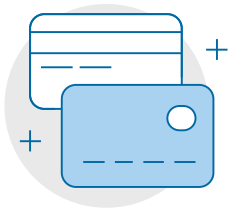
		Page
1	Fundamentals of credit card processing	1
2	Risk management and data security	6
3	PCI compliance	18
4	**Trends in payments**	**25**

Long-term trends in U.S. payments



Card growth potential

U.S. credit and debit card volume of $7 trillion[1] amounts to roughly half of all U.S. consumer expenditures[2]



Ongoing tender share shift

Consumers continue to prefer debit cards and credit cards over cash[3]

Increasing share of e-commerce

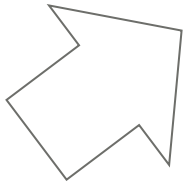
As of Q1 2020, e-commerce accounted for 11.8% of total U.S. retail payments[4]

Substantial growth of m-commerce

Mobile is approximately 1/3 of total e-commerce spend, and continues to grow[5]

Online fraud

As the in-store point of sale has become more secure through EMV, fraudsters are moving online



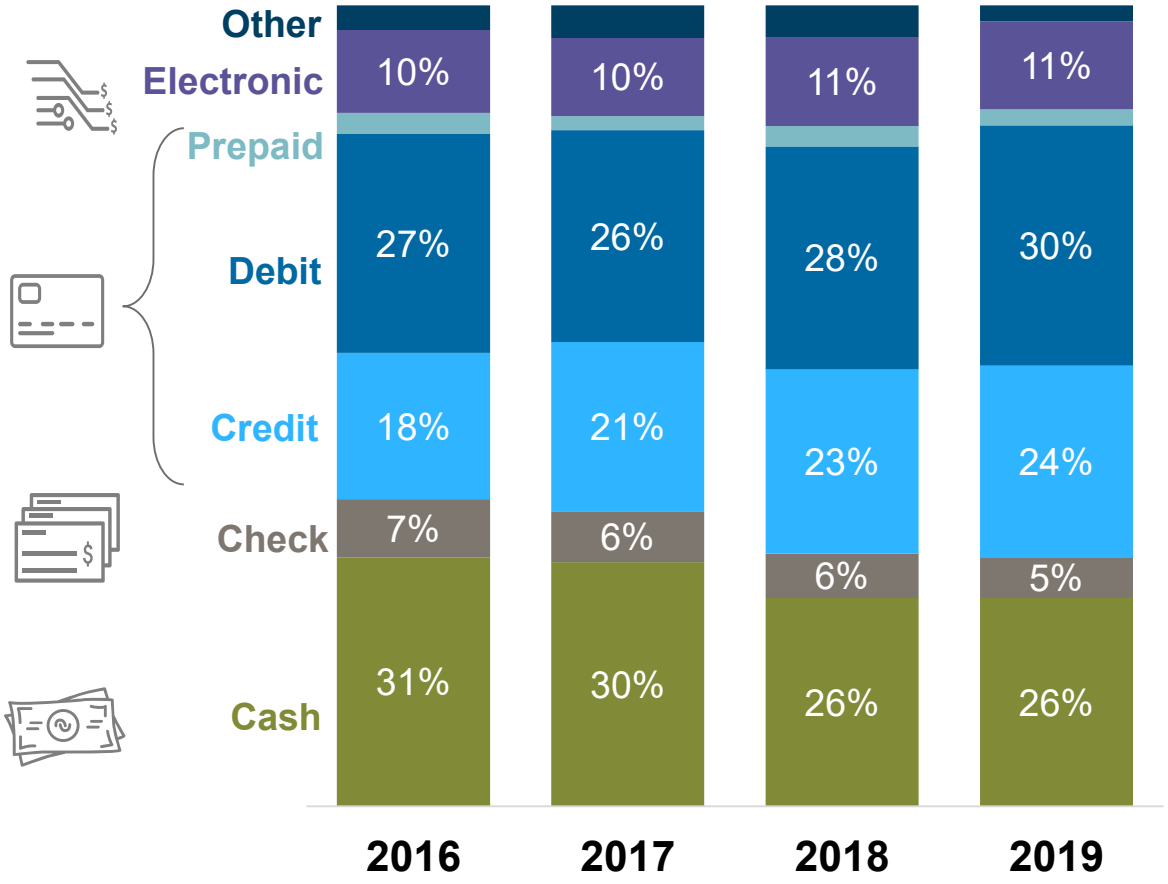
Covid-19 Impacts

Covid-19 has accelerated pre-existing payments-related trends

[1] Federal Reserve Payments Study, December 2018.
[2] Consumer spending totaled $14.6 trillion in Q1 2020, according to the U.S. Bureau of Economic Analysis.
[3] Federal Reserve Bank of San Francisco, June 2019.
[4] U.S. Census Bureau News, Q1 2020. Estimates adjusted for seasonal variation, trading-day differences and moving holidays.
[5] Comscore, Q1 2020 Emerging Digital Payments Advisor

Share shift: sharp uptick in credit usage over past several years

Share of payment instrument usage by year



Source: Federal Reserve Bank of San Francisco, July 2020

Factors driving higher credit use

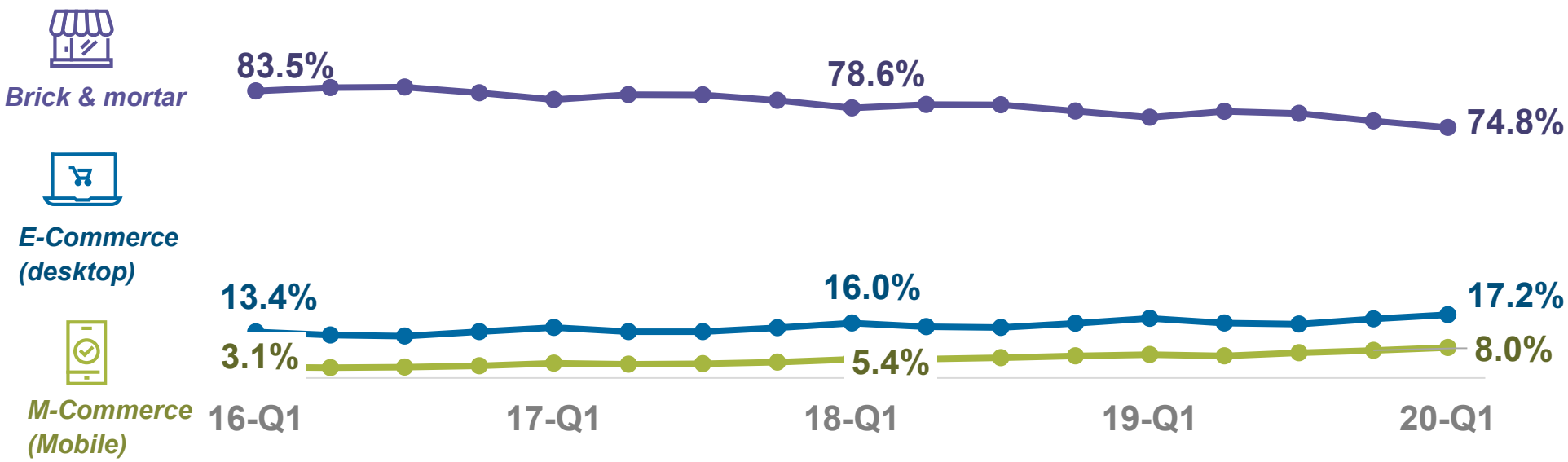
- Increased value of **merchant rewards programs** tied to proprietary credit programs[1]
- **Improving FICO scores** of population and greater access to credit[2]
- **Higher levels of credit** extended to individuals and rise in number of credit card accounts[3]

1 Fool.com, Why Your Credit Card Rewards Could be in Danger, November 9, 2019
2 Marketwatch, One Reason Credit Scores are Rising, September 15, 2019
3 Federal Reserve, Consumer Credit Report – G19, September 2019

J.P.Morgan

E-Commerce & M-Commerce: nearly 25% of US retail spend

Share of U.S. retail spend



Factors Driving E-Commerce and M-Commerce Growth

- **2-day, 1-day and same-day delivery**
- **Growth of marketplaces**
- **Mobile-first investments**
- **Integrated retail channels**
- **Broadband penetration**

Source: comScore, Q1 2020 Emerging Digital Payments Advisor (EDPA)

J.P.Morgan

10 COVID-19 consumer payment trends

1. **A substantial increase in e-commerce purchases**
   E-commerce is one of the few verticals that has grown during the crisis

2. **Increase in contactless payments at the point of sale**
   The U.S. had been behind several other countries in contactless adoption, but is now catching up; many consumers are experiencing contactless payments for the first time

3. **Increase in chargebacks**
   Frustrated consumers are resorting to chargebacks when they can't reach a representative, and as a solution to financial distress

4. **Reduced access to credit**
   Some issuers are reassessing credit lines, and by one estimate 50 million Americans have had credit lines reduced or eliminated

5. **Sharp drop in credit card spend**
   Credit card spend has declined due to the reduction in available credit and consumers' hesitancy to incur debt

6. **Increase in income due to governmental programs**
   Temporary governmental assistance actually boosted income substantially, but uncertainty is ahead

7. **Highest consumer savings rate in recorded U.S. history**
   The high savings rate is a result of an influx of government cash assistance and consumers bunkering down

8. **Greater interest in buy now, pay later options**
   Some alternative financing options like Afterpay, Affirm and Klarna are reporting strong growth

9. **A pause in the backlash against no-cash stores**
   Pre-crisis, several local jurisdictions had implemented regulations requiring businesses to accept cash; this trend has been at a minimum paused, as consumers adopt touchless payments experiences and perceptions of cash have changed

10. **Integrated channel experiences**
    Integrated channels – aka omnichannel – have made possible payment experiences that consumers are flocking towards (e.g., buy online, pick up in store)

Sources:
Oliver Wyman, Payments Shifts With COVID-19, April 2020
Business Insider, Why merchants are betting on buy now pay later to boost sales, April 8, 2020
Business Insider, Why Affirm CEO Max Levchin is eyeing growth amid the coronavirus, April 29, 2020

Contactless cards

U.S. adoption

40% increase in Visa contactless usage year-over-year.

55% of consumers expect to use contactless cards more often

60% of consumers are confident that contactless payments were safer in terms of the spread of COVID-19.

Source: Visa, Purchasing in a Pandemic, 2020

U.S. readiness

8 **Of the top 10** merchants accept **tap to pay**

69% Of face-to-face transaction **take place at tap-to-pay merchants**

300M **Tap to pay cards issue** by the end of 2020

Visa 2020 Investor Presentation

Getting ready for contactless

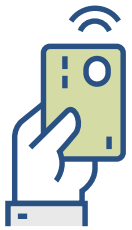
Contactless payments have quickly become a must-have for shops, restaurants and businesses across the country. What started for many to promote safety has evolved into an important tool to build profit and efficiency.

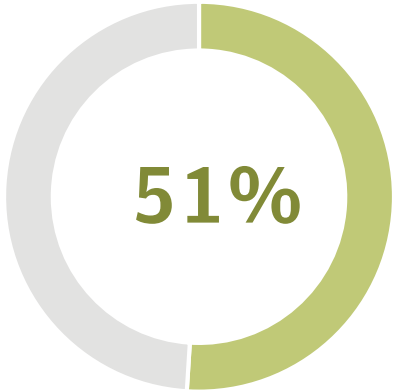
80% of survey consumers are concerned about touching a payments reader[1]

51% of consumers report using contactless payments[2]

70% who are new to contactless payments report they will continue after the pandemic[1]

54% of U.S. consumers would switch to a new store that installed contactless payments[3]





Consumers reporting usage of contactless payments[2]

Check your equipment to see whether it's already capable of accepting contactless payments. If you see three lines that look like the Wi-Fi symbol tipped on its side, you're ready to go.

[1]Payments Journal (NFC cards, smartphones, and wearables), [2] CBNC, Mastercard survey, [3]The Visa Back to Business Study, Global Small Business and Consumer Insights, July 2020

Polling Question #6

Invisible payments: U.S. and overseas implementations

Asia is ahead in this area, but the U.S. is expected to catch up

Notable implementations in Asia

Smile to pay

Hand scanning

Facial recognition

U.S. implementations

- Giant Eagle / Grabango[1]
- Amazon Go[2]
- Amazon Fresh - Dash Cart[3]
- Dunkin / Mastercard[4]
- White Castle / Mastercard[5]
- Circle K / Standard Cognition[6]

[1]Supermarket News, Giant Eagle Goes Live, September 1, 2020
[2]Amazon.com web page, as of July 29, 2020
[3]Amazon.com, Fresh web page, as of September 21, 2020
[4]Payments Journal, Dunkin' and Mastercard Brew up Autonomous Checkout, September 8, 2020
[5]Hospitality Technology, White Castle to Pilot Vehicle Recognition Technology, September 2, 2020
[6]Forbes, Cashierless Technology is Coming, August 11, 2020

Streamlining your operations

Merchant processing optimization (for illustrative purposes only)

Current state

Decentralized collection points across the organization

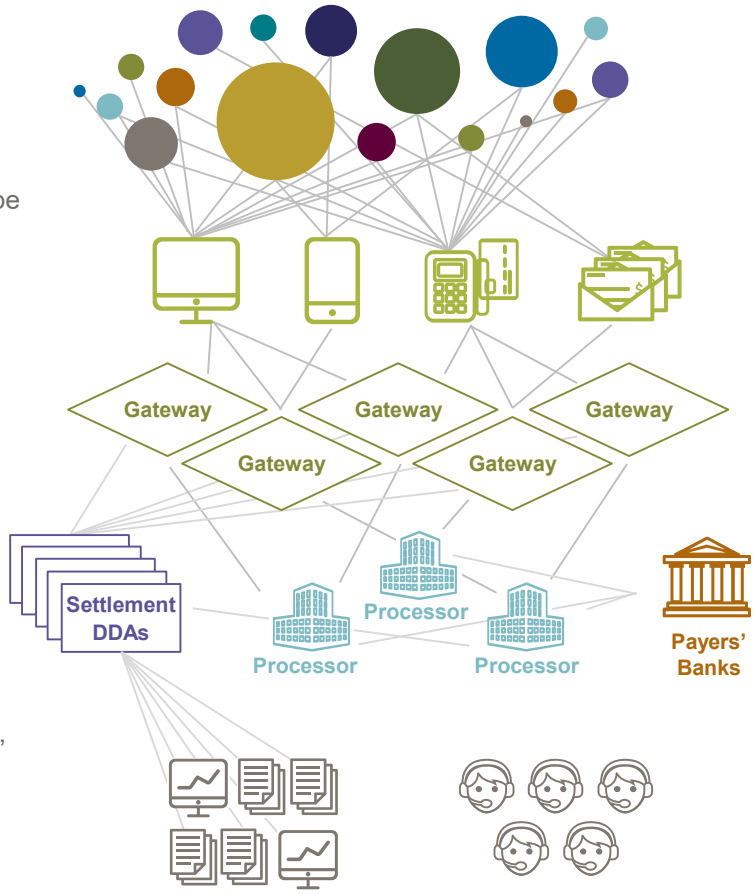
Complex vendor landscape across card collection channels

Multiple back-end processors

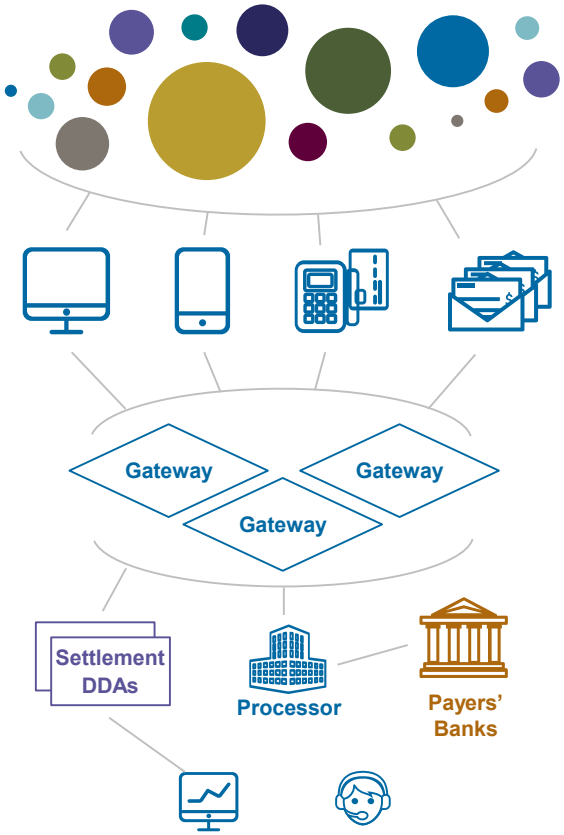
Fragmented settlement across multiple merchant accounts and DDAs

Siloed reports and portals, manual reconciliation

Separate service teams, depending on provider



Future state



One integrated, omnichannel platform – streamline connectivity, reporting, and service

J.P.Morgan