PaymentsEd

Your source for payments education

Payments Fundamentals

Matt Leman

Stephanie Meyers

PaymentsEd Forum

In 2025, U.S. consumers used credit cards to purchase more than $3.8 trillion worth of goods and services.[1]

Cards are powering mobile, online, in-store and even biometric payments.

[1] https://www.emarketer.com/content/three-biggest-credit-card-trends-of-2025

The basic elements of a card transaction

Whether a payment is made at the point of sale, online or via mobile device, the fundamentals of a card transaction are the same.

Authorization

Confirms sufficient funds and updates authorization amount unavailable for other purchases

Clearing & Settlement

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

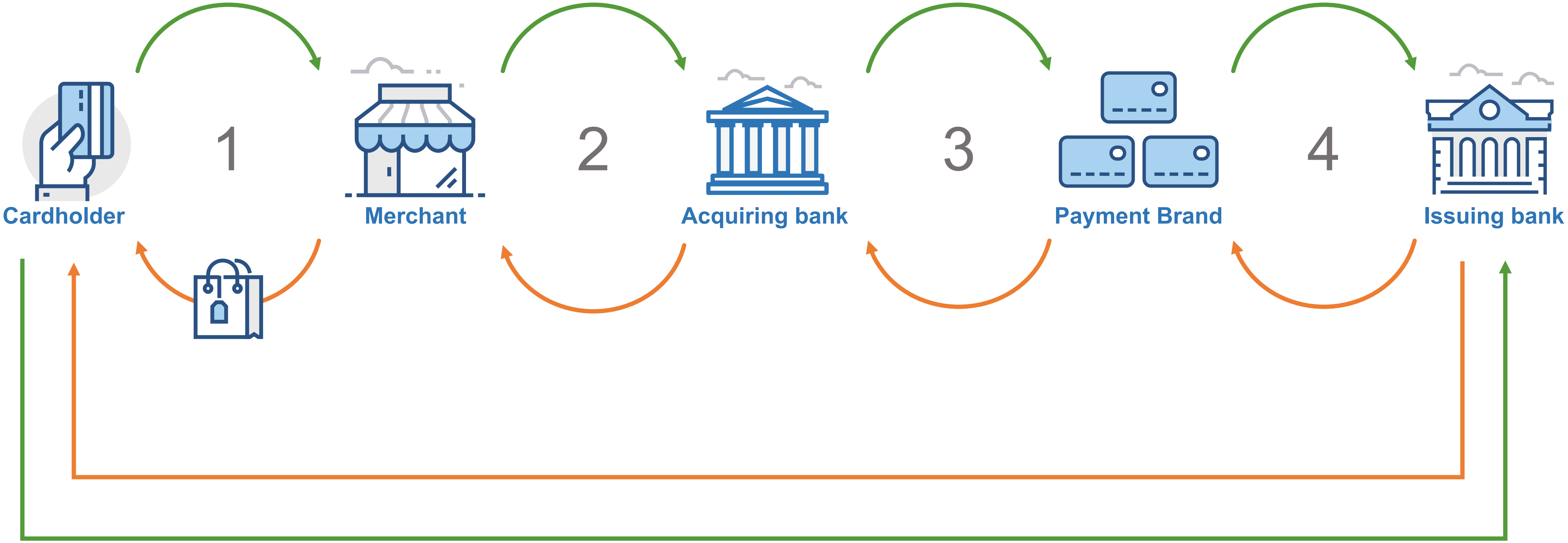
Settlement: Issuing bank sends payment to the payment network, which in turns sends payment to the merchant acquirer

Funding

Acquirer pays the merchant for their activity

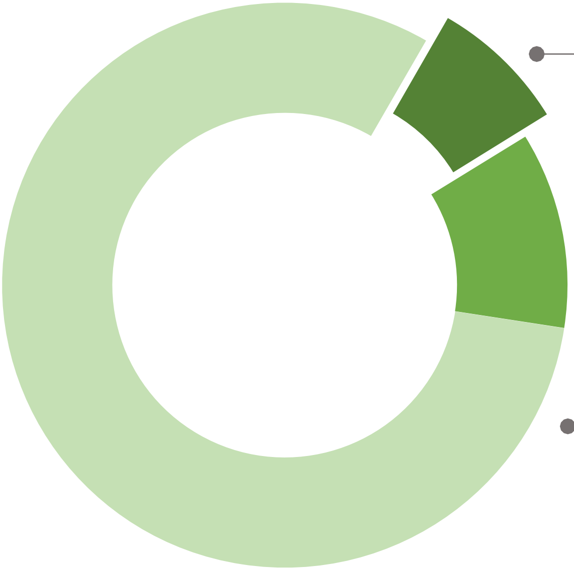
The traditional card transaction flow

Illustrative



What makes up a transaction fee?

Card transactions are subject to processor, network and interchange fees. The relative size of representative fees are depicted below.



Processor fee
Assessed by a merchant services provider for coordinating authorization, settlement, disputes, reporting and customer service

Network 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

Interchange fees, managed and assessed by the payment brands, create incentives that help to ensure the reliability and security of card transactions for merchants and consumers.

Qualifying transactions for optimal interchange rate

Card type, transaction type, payment processing method and business classification can all influence the interchange fee rates.

To help qualify transactions for optimal interchange rate

- **Use the most secure authorization method**
  - Insert chip or tap – avoid manual key entry
- **Capture Level II and Level III data (or Commercial Enhanced Data)**
  - Additional information helps to mitigate risk in the eyes of the payment brands

Qualifying transactions for optimal interchange rate

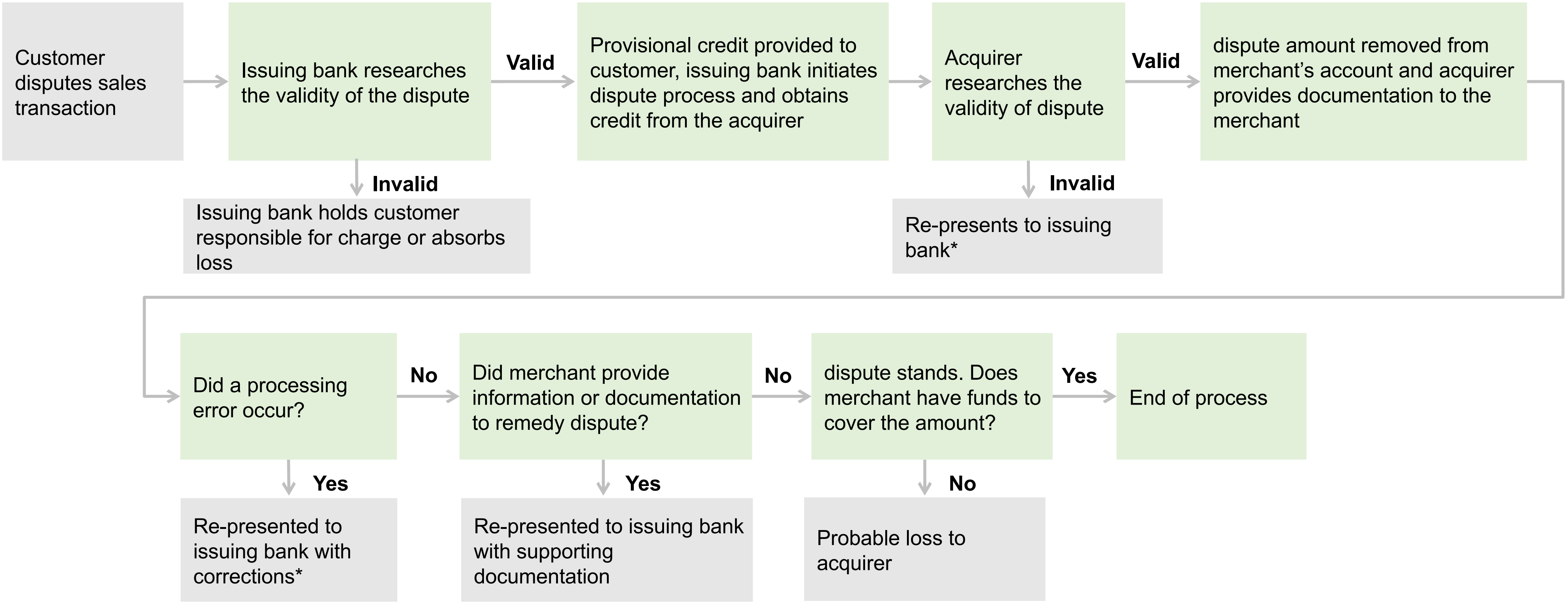
Card type, transaction type, payment processing method and business classification can all influence the interchange fee rates.

To help qualify transactions for optimal interchange rate

- **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

How do disputes work?

A representative dispute process



*The payment brands act as a payment clearinghouse between the issuing bank and acquiring bank during the dispute and re-presentment process. A compliance resolution process also exists at the bank card association if no dispute rights are available to the issuing bank and a financial loss is incurred as a result of bank card association rules. A second dispute may occur if the re-presentment is invalid, documentation did not support the charge or another dispute reason code applies. If the acquirer disputes the second dispute presentment, the acquirer may file an appeal for arbitration with the bank card association. Re-presentment is not allowed for a second dispute

PCI compliance overview

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.

PCI DATA SECURITY STANDARD – HIGH-LEVEL OVERVIEW	
Build and maintain a secure network and systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect account data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a vulnerability management report	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement strong access control measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an information security policy	12. Support information security with organizational policies and programs

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

PCI compliance is a journey

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.***

People

Hire qualified and trusted partners and train your staff to understand payment data security essentials.

Process

Put the right policies and practices in place to make payment security a priority every day.

Technology

Make sure you are using the right technology and implementing it correctly to get the best security and business benefits.

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

Protect data at every step with comprehensive data security

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.

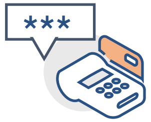
Tokenization
Protect data while at rest by replacing payment data with a secure token that cannot be converted back to card or account information within your network.

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.

Disclaimer

This material was prepared exclusively for the benefit and internal use of the J.P. Morgan client to whom it is directly addressed (including such client's subsidiaries, the "Company") in order to assist the Company in evaluating a possible transaction(s) and does not carry any right of disclosure to any other party. In preparing this material, 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. This material is for discussion purposes only and is incomplete without reference to the other briefings provided by J.P. Morgan. Neither this material nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

J.P. Morgan, JPMorgan, JPMorganChase, Chase, Chase Merchant Services, and Chase Payment Solutions are marketing names for certain businesses of JPMorganChase and its subsidiaries worldwide (collectively, "JPMC"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMC entities. JPMC contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorgan", "JPMorganChase", "Chase", "Chase Merchant Services" and "Chase Payment Solutions" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMC of any product or service which would be unlawful under applicable laws or regulations.

Investments or strategies discussed herein may not be suitable for all investors. Neither J.P. Morgan nor any of its directors, officers, employees or agents shall incur in any responsibility or liability whatsoever to the Company or any other party with respect to the contents of any matters referred herein, or discussed as a result of, this material. This material is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters.

Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates. This material does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other products or services and J.P. Morgan reserves the right to withdraw at any time. All products and services are subject to applicable laws, regulations, and applicable approvals and notifications. The Company should examine the specific restrictions and limitations under the laws of its own jurisdiction that may be applicable to the Company due to its nature or to the products and services referred herein.

Any mentions of third-party trademarks, brand names, products and services are for referential purposes only and any mention thereof is not meant to imply any sponsorship, endorsement, or affiliation. Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to, and superseded by, the terms of separate legally binding documentation and/or are subject to change without notice. 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 Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured. Non-deposit products are not FDIC insured. JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.