PAYMENT PROCESSING ARRANGEMENTS FOR MERCHANTS 101:

PRESENTATION FOR

THE ASSOCIATION OF CORPORATE COUNSEL

JOANN CARLTON
SUZANNE GAINEY
KATHERINE LAMBERTH

February 18, 2021

Agenda

- Players in the Payment Processing Space
- Card Network Rules and PCI DSS
- Card Network Fees
- Card Network Charges and Fines
- Negotiating Payment Processing Agreements

PLAYERS IN THE PAYMENT PROCESSING SPACE

Payment Processing During the Pandemic

Basic Payment Processing Lifecycle

Cardholder

Merchant

Acquiring Bank

Issuing Bank

Card Networks

Typical Players in Payment Processing

- **Cardholder** – the individual initiating the purchase by providing a payment method either in person (a "card present" transaction) or remotely (a "card not present" transaction).

- **Merchant** – the entity from which the cardholder is making a purchase. The merchant will make available the method for accepting payment (*e.g.*, a point-of-sale device).

- **Acquiring Bank (Acquirer/Merchant Acquirer)** – financial institutions that maintain merchant accounts and that pass transaction requests and data between merchants and Card Networks. The acquiring bank settles transactions into the merchant account for a particular merchant.

Typical Players in Payment Processing

- **Card Networks (Card Associations/Card Brands)** – these are the governing bodies of payment processing. The Card Networks connect everyone in the payment processing system and set interchange fees, mediate disputes, establish the specific rules for processing, *etc*.

- **Issuing Bank (Issuer)** – financial institution that issues the credit card to the cardholder and facilitates funding of transactions.

Additional Players in Payment Processing

- **Payment Processors** – companies that process payment card transactions on behalf of merchants and their acquiring bank. Payment processors often offer additional services that complement payment processing services. Sometimes the payment processor and the acquiring bank are one and the same.

- **Independent Sales Organizations (ISOs)** – are not officially part of the Card Networks, but typically have partnerships with acquiring banks to provide services to merchants (*e.g.*, payment gateways, analytics, *etc.*). Typically, ISOs resell payment processing services offered by a processor (*i.e.*, a processor can be an ISO, but an ISO cannot be a processor).

CARD NETWORK RULES AND PCI DSS

Card Network Rules

- Each Card Network has its own set of rules that must be followed by the Card Network's members.
- Card Network Rules are long and complex:
  - Visa's Core Rules and Product and Service Rules are 892 pages long.
  - Mastercard's most recent Mastercard Rules are 403 pages long.
- Each Card Network can modify its Card Network Rules at any time.

PCI DSS

- The Payment Card Industry Data Security Standard ("**PCI DSS**") sets forth minimum technical and operational requirements for the protection of cardholder data.

- PCI DSS version 1.0 was originally adopted by Visa, Mastercard, Discover, American Express and Japan Credit Bureau (JCB) in December 2004. In 2006, these five major payment card brands formed the PCI Security Standards Council, which has administrative responsibility over PCI DSS.

- PCI DSS version 3.2.1 became effective in May 2019 and version 4.0 is expected in mid-2021.

- PCI DSS applies to ***all*** entities involved in payment card processing – ***including merchants***!

PCI DSS – The Basic Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall to protect cardholder data 2. Do not use vendor supplied password defaults.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt cardholder data across open public networks.
Maintain a Vulnerability Management Program	5. Protect systems against Malware and update anti-virus software. 6. Develop and maintain security systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data on a need to know basis. 8. Identify and authenticate access to systems 9. Restrict physical access to cardholder data.
Regularly monitor and test networks	10. Tract and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain and Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

PCI DSS – Enforcement Through Contract

- Merchants are generally bound by PCI DSS through their merchant processing agreements.

- The Card Networks have established different merchant categories that govern the level of PCI compliance monitoring that is required:

  - **Level 1** – merchants that process over 6 million card transactions annually.
  - **Level 2** – merchants that process between 1 million and 6 million transactions annually.
  - **Level 3** – merchants that process between 20,000 and 1 million transactions annually.
  - **Level 4** – merchants that process less than 20,000 transactions annually.

- A merchant's failure to comply with PCI DSS can result in ***fines*** or the ***loss of the ability to accept card payments***.

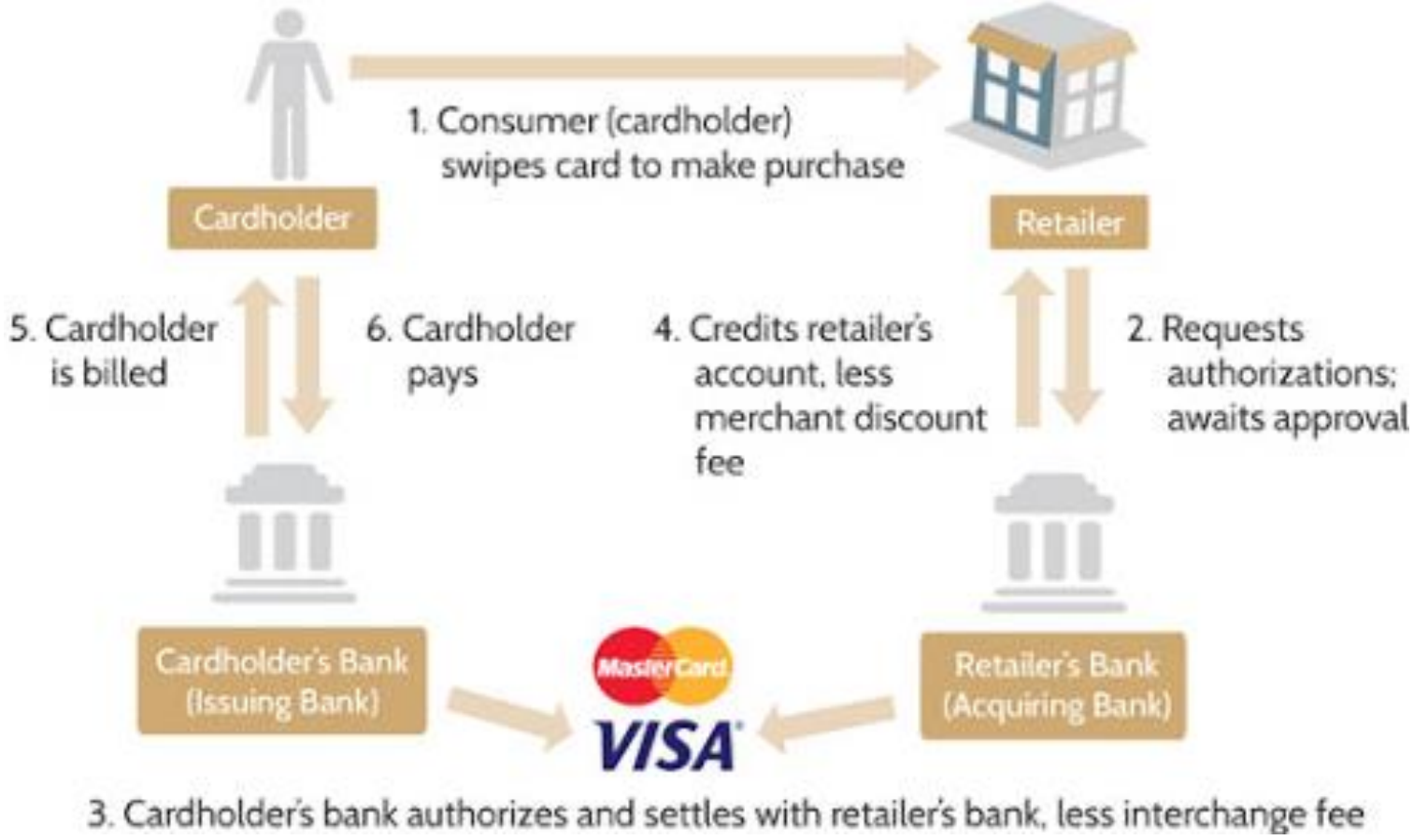
CARD NETWORK FEES

Interchange Fees

What is an Interchange Fee?

- For each transaction, an interchange fee is a fee paid from the acquiring bank (merchant's bank) to the issuing bank (cardholder's bank).
- Amount is set by card networks (*e.g.*, Visa and Mastercard) but is designed to compensate issuers.
- The interchange fee is part of the "merchant discount" or rate charged to the merchant on each transaction, which also includes processing fees (paid to acquirer) and assessment fees (paid to card network).
- The applicable interchange fee may vary by transaction, and depends on the type of good or service and nature of the transaction (*e.g.*, in-person vs. card not present transactions).

Transaction Illustration



Payment Card Surcharges

What is a Surcharge?

- Prohibited by card networks until 2013, a surcharge is an additional fee that a merchant may add to the price that a cardholder pays for goods or services when the cardholder uses a credit card for payment, instead of another form of payment.
- In the U.S., surcharges may only be applied on credit card transactions and cannot exceed the greater of the merchant discount rate or 4%.
- May apply at the “brand level” or “product level”.
- For merchants that accept credit cards from more than one card network, the surcharge must be applied on same terms and conditions as any equal or higher cost competitor.

Requirements and Considerations

- Is the surcharge legal under applicable law?
  - Prohibited in Colorado, Connecticut, Kansas, Maine, Massachusetts, and Oklahoma.
  - Potentially prohibited in California, Florida, New York, Texas, and Utah – statutes have been found unconstitutional "as applied".
  - Such statutes do not necessarily prohibit Merchant Discounts (but see Florida, Kansas, Maine, Texas).
- Has 30 days notice been provided to card network(s) and acquirer(s)?
- Is surcharge properly disclosed to customers?
  - For both in-store and online transactions, must be disclosed at the point of entry and point of sale.
  - For every transaction, the receipt must separately identify the final surcharge amount (must be itemized on receipt).

CARD NETWORK CHARGES AND FINES

Chargebacks

What is a Chargeback?

- A chargeback occurs if there is a “dispute” regarding a transaction under the card network rules, pursuant to which an issuing bank may return a transaction to an acquirer for reimbursement and where the merchant is liable for the reimbursement.
- A chargeback can fall under the following dispute categories:
  - Fraud (as applicable)
  - No Authorization/ Error (as applicable)
  - Consumer Dispute
- Acquirer will apply funds maintained in the merchant’s reserve account to chargebacks.

Chargebacks – Fraud

- Under the card network rules, “fraud” includes unauthorized use by a person of a credit card or debit card (*i.e.*, person’s use not authorized by cardholder).
  - A cardholder is liable for fraud if:
    - The cardholder was fraudulent or negligent in the handling of the credit card or debit card, or account information.
    - The cardholder participated in the transaction.
  - An issuing bank is liable for fraud if:
    - For in-person transactions that are either (i) conducted at an EMV-compliant device, is Chip-initiated, and otherwise correctly processed, or (ii) the transaction is authorized by the issuing bank and it is identified as a fallback transaction in the authorization message.
    - For card not present transactions, the transaction was properly authenticated (pursuant to CAVV or security procedures) pursuant to applicable requirements under card network rules.
  - An acquirer is liable for fraud if in-person or card not present transactions are not conducted pursuant to applicable requirements under network card rules, which may be in turn allocated to merchant as applicable.

Chargebacks – Consumer Dispute

- Regardless of merchant policy, a cardholder may dispute a transaction resulting in a chargeback for the following reasons:
  - The transaction was for goods or services not received because the merchant was unwilling or unable to provide the goods or services.
  - The transaction was a recurring transaction processed after the customer withdrew permission or had account closed.
  - The transaction was for goods or services that were (i) not as described (did not match what was described on record presented at time of purchase), (ii) damaged or defective, or (iii) subject to dispute of quality by the cardholder.
  - The transaction was for counterfeit goods.
  - The terms of the transaction were misrepresented to the cardholder – ***always*** applies for transactions involving certain goods or services including timeshares, debt consolidation and settlement services.
  - The transaction for goods or services was cancelled by the cardholder.

Merchant Penalties and Fines

- The card network rules subject merchants to fines or other penalties (including enhanced compliance procedures and, ultimately, disqualification) for elevated fraud or elevated chargebacks.
- Elevated Fraud Program:
  - For example, Visa monitors merchants for an elevated level of fraud categorized as:
    - Standard (exceeds $75,000 fraud amount and 0.9% fraud-dollar-to-sales per month)
    - High-risk (applies to certain merchant categorization categories)
    - Excessive (exceeds $250,000 fraud amount and 1.8% fraud-dollar-to-sales ratio per month)
  - Visa will require appropriate fraud remediation tools and mitigation measures to be instituted and assess non-compliance assessments as applicable.
- Elevated Chargeback Program:
  - For example, MasterCard classifies an excessive chargeback merchant as a merchant that has at least 100 chargebacks and a 1.5% chargeback-to-transaction ratio for two consecutive months.

NEGOTIATING PAYMENT PROCESSING AGREEMENTS

Negotiating Processing Agreements

Operational vs. Commercial Terms

- Merchants will have more ability to negotiate provisions that are ***commercial*** in nature rather than ***operational***.

- Keep in mind that certain provisions are required to be passed down to merchants by the Card Networks or others – these are typically ***not*** negotiable.

Key Provisions to Review

- **Reserve Accounts** – set forth the circumstances under which a reserve account may be established, and what amount can be deposited into the reserve accounts.
- **Chargebacks** – ensure that the processor or acquiring bank cooperates with the merchant in any chargeback dispute.
- **Information Security Obligations** – most processing agreements will not impose information security obligations on the processor or acquiring bank; however, it is possible to get some basic protections in the agreement, including a promise to comply with PCI DSS.

Key Provisions to Review (continued)

- **Fees** – ensure that the fees are clearly set forth in the agreement, and that the merchant understands all fees. Also, watch out for sneaky fees!
- **Exclusivity** – many processing agreements will include an exclusivity provision. Depending on the merchant, this may not make sense (*e.g.*, if the merchant has multiple locations and uses different processors in different regions).
- **Termination Rights** – review the termination rights of all parties. Typically, each party will have a right to terminate for convenience; however, often additional termination fees will apply for early termination.

Key Provisions to Review (continued)

- **Obligations Upon Termination** – determine the merchant's obligations when the agreement terminates (*e.g.*, return of equipment) and ensure the merchant can comply. Often, additional fees apply for failure to comply.
- **Indemnities** – the merchant will always be asked to indemnify the processor/acquiring bank. The processor/acquiring bank will also usually agree to provide certain indemnities (*e.g.*, IP infringement, non-compliance with law or card network rules).
- **Liability Caps** – the processor/acquiring bank will try to limit its liability as much as possible, but merchants may have some ability to increase the amount of the caps.

MVA Contacts

SUZANNE K. GAINEY
Associate

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

suzannegainey@mvalaw.com
T: (704) 331-3559 F: (704) 378-1959

KATHERINE M. LAMBERTH
Associate

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

katherinelamberth@mvalaw.com
T: (704) 331-3554 F: (704) 378-2073