Unit 3: Electronic Payment System (9 Hrs.)

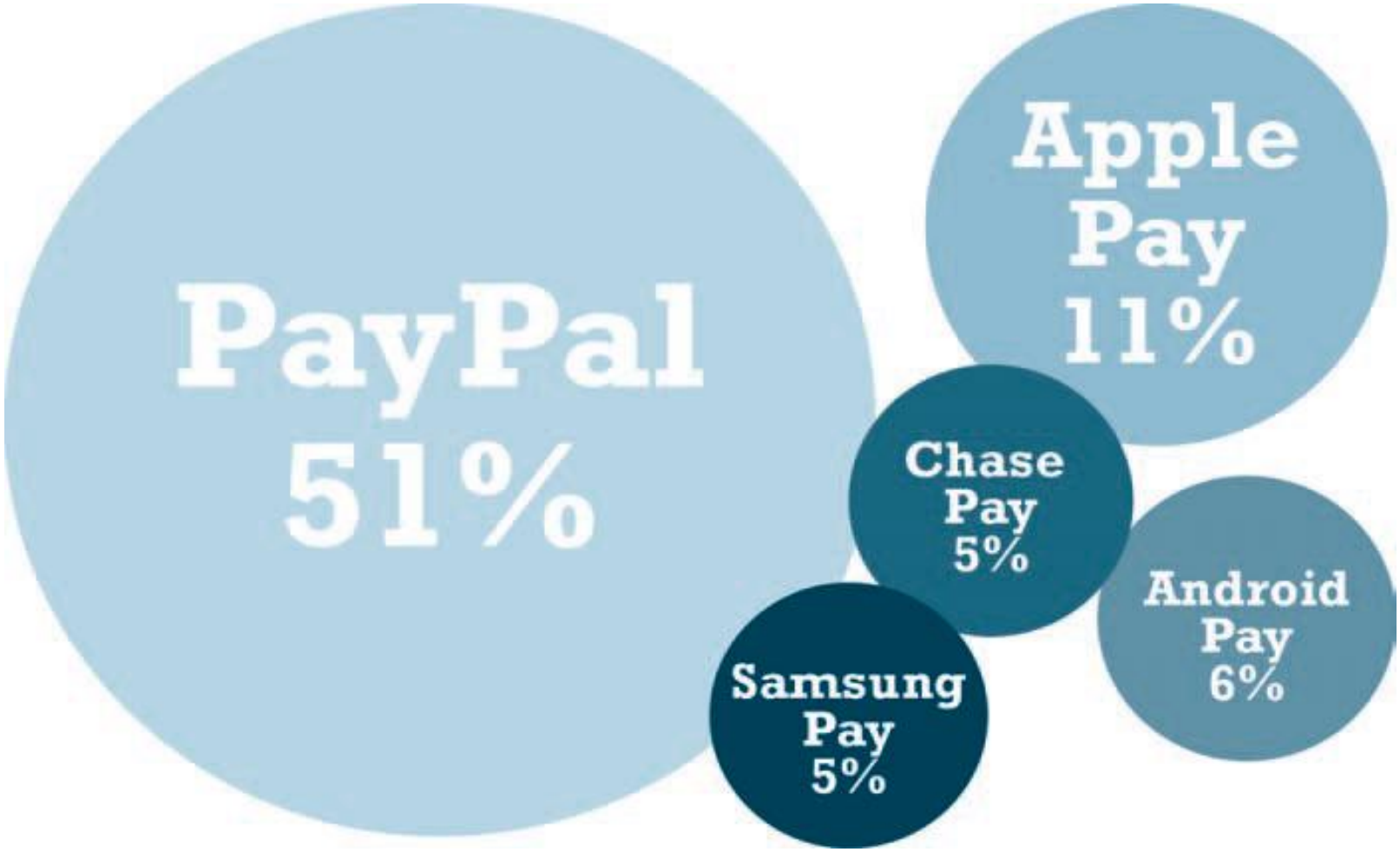
Introduction

- For the most part, existing payment mechanisms such as cash, credit cards, debit cards, checking accounts, and stored value accounts have been able to be adapted to the online environment, albeit with some significant limitations that have led to efforts to develop alternatives.
- In addition, new types of purchasing relationships, such as between individuals online, and new technologies, such as the development of the mobile platform, have also created both a need and an opportunity for the development of new payment systems.
- In this section, we provide an overview of the major e-commerce payment systems in use today.

MAJOR TRENDS IN E-COMMERCE PAYMENTS 2016–2017

- Payment by credit and/or debit card remains the dominant form of online payment.
- Mobile retail payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, Samsung, and PayPal extend their reach in mobile payment apps.
- Large banks enter the mobile wallet and P2P payments market.
- Square gains further traction with a smartphone app, credit card reader, and credit card processing service that permits anyone to accept credit card payments.
- Google refocuses Google Wallet, which had met with tepid response, solely on sending and receiving money.
- Mobile P2P payment systems such as Venmo take off.

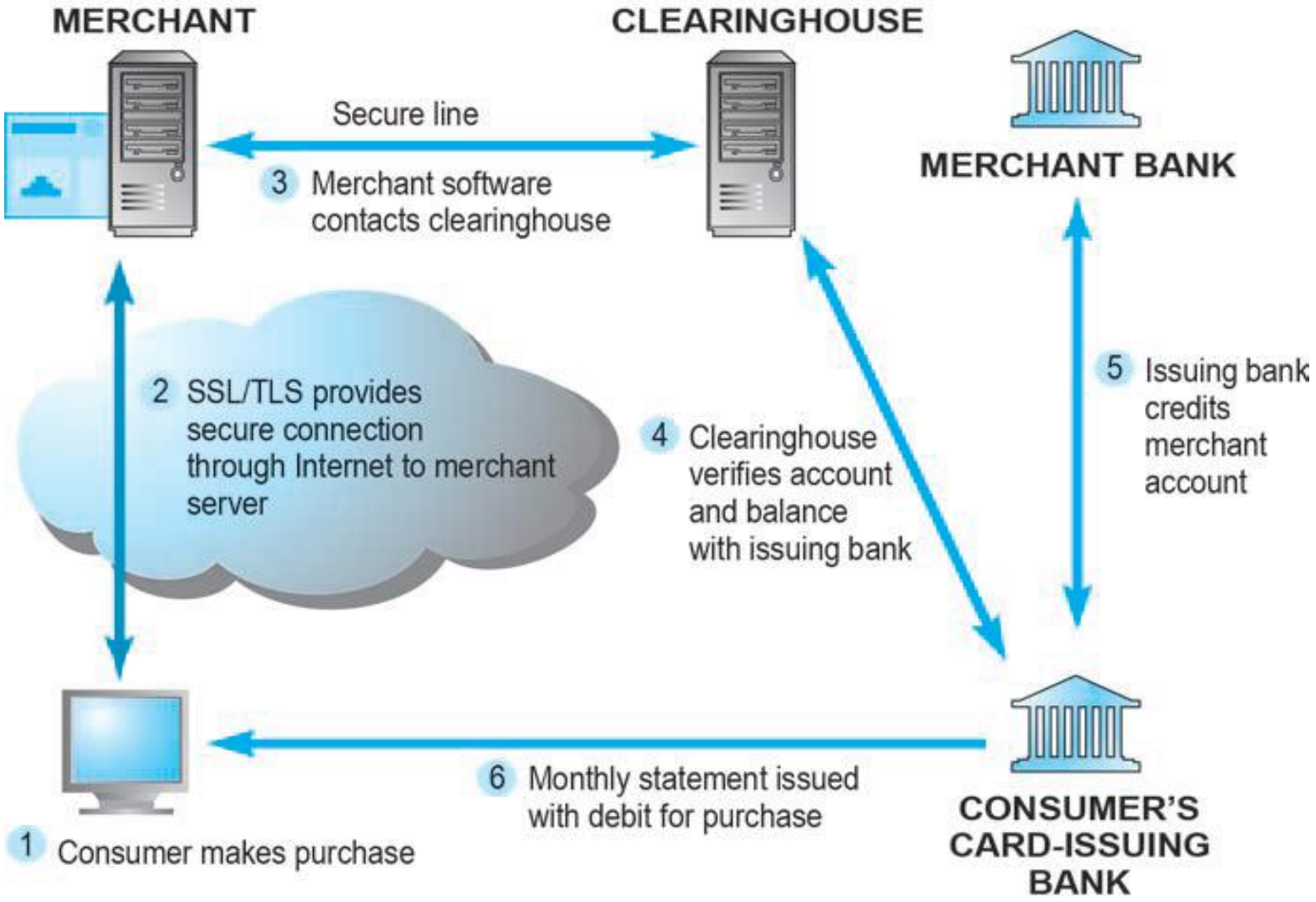
ALTERNATIVE PAYMENT METHODS USED BY U.S. CONSUMERS



ONLINE CREDIT CARD TRANSACTIONS

- Because credit and debit cards are the dominant form of online payment, it is important to understand how they work and to recognize the strengths and weaknesses of this payment system.
- Online credit card transactions are processed in much the same way that in-store purchases are, with the major differences being that online merchants never see the actual card being used, no card impression is taken, and no signature is available.
- Online credit card transactions most closely resemble Mail Order-Telephone Order (MOTO) transactions.
- These types of purchases are also called Cardholder Not Present (CNP) transactions and are the major reason that charges can be disputed later by consumers.
- Because the merchant never sees the credit card, nor receives a hand-signed agreement to pay from the customer, when disputes arise, the merchant faces the risk that the transaction may be disallowed and reversed, even though he has already shipped the goods or the user has downloaded a digital product.

HOW AN ONLINE CREDIT CARD TRANSACTION WORKS



- A **merchant account is simply a bank account that allows companies to process credit card payments** and receive funds from those transactions.
- (1). When a consumer wants to make a purchase, he or she adds the item to the merchant's shopping cart. When the consumer wants to pay for the items in the shopping cart, a secure tunnel through the Internet is created using SSL/TLS (Socket Secure Layer/Transport Layer Security).
- Using encryption, SSL/TLS secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet (2).
- SSL does not authenticate either the merchant or the consumer. The transacting parties have to trust one another. Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse (3).
- As previously noted, a clearinghouse is a financial intermediary that authenticates credit cards and verifies account balances. The clearinghouse contacts the issuing bank to verify the account information (4).
- Once verified, the issuing bank credits the account of the merchant at the merchant's bank (usually this occurs at night in a batch process) (5).
- The debit to the consumer account is transmitted to the consumer in a monthly statement (6).

Credit Card E-commerce Enablers

- Companies that have a merchant account still need to buy or build a means of handling the online transaction; securing the merchant account is only step one in a two-part process.
- Today, Internet payment service providers (sometimes referred to as payment gateways) can provide both a merchant account and the software tools needed to process credit card purchases online.
- For instance, Authorize.net is an Internet payment service provider.
- The company helps a merchant secure an account with one of its merchant account provider partners and then provides payment processing software for installation on the merchant's server.
- The software collects the transaction information from the merchant's site and then routes it via the Authorize.net "payment gateway" to the appropriate bank, ensuring that customers are authorized to make their purchases.
- The funds for the transaction are then transferred to the merchant's merchant account.
- CyberSource is another well-known Internet payment service provider.

PCI-DSS Compliance

- The **PCI-DSS (Payment Card Industry-Data Security Standard) is a data security** standard instituted by the five major credit card companies (Visa, MasterCard, American Express, Discover, and JCB).
- PCI-DSS is not a law or governmental regulation, but an industry-mandated standard.
- Every online merchant must comply with the appropriate level of PCI-DSS in order to accept credit card payments.
- Those that fail to comply and are involved in a credit card breach may ultimately be subjected to fines and other expenses.
- PCI-DSS has various levels, related to the number of credit and/or debit cards processed by the merchant each year.
- Level 1, the strictest level, applies to very large merchants that process more than 6 million transactions a year, while Level 2 applies to those who process between 1 million and 6 million.
- Level 3applies to organizations that process between 20,000 and 1 million transactions, while Level 4 applies to smaller merchants that process less than 20,000 transactions.

- PCI-DSS has six major control objectives.
- It requires the merchant to (a) build and maintain a secure network, (b) protect cardholder data, (c) maintain a vulnerability management program, (d) implement strong access control measures, (e) regularly test and monitor networks, and (f) maintain an information security policy.
- Each of these six broad control objectives has further specific requirements that must be met.
- The most current version of PCI-DSS is Version 3.1, which went into effect as of April 2015 (PCI Security Standards Council, 2015).

Limitations of Online Credit Card Payment Systems

- The most important limitations involve security, merchant risk, administrative and transaction costs, and social equity.
- The existing system offers poor security. Neither the merchant nor the consumer can be fully authenticated.
- The merchant could be a criminal organization designed to collect credit card numbers, and the consumer could be a thief using stolen or fraudulent cards.
- The risk facing merchants is high: consumers can repudiate charges even though the goods have been shipped or the product downloaded.
- The banking industry attempted to develop a secure electronic transaction (SET) protocol, but this effort failed because it was too complex for consumers and merchants alike.
- As banks switch to EMV (Europay, Mastercard, Visa) cards with computer chips, offline credit card fraud becomes more difficult, encouraging criminals to focus on online fraud.
- The administrative costs of setting up an online credit card system and becoming authorized to accept credit cards are high.
- Transaction costs for merchants also are significant—roughly 3% of the purchase plus a transaction fee of 20–35 cents per transaction, plus other setup fees.
- Credit cards are not very democratic, even though they seem ubiquitous.
- Millions of young adults do not have credit cards, along with millions of others who cannot afford cards or who are considered poor risks because of low incomes.

ALTERNATIVE ONLINE PAYMENT SYSTEMS

- The limitations of the online credit card system have opened the way for the development of a number of alternative online payment systems.
- Chief among them is PayPal.
- PayPal (purchased by eBay in 2002 and then spun-off as an independent company again in 2015) enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit. Paypal is an example of an **online stored value payment system, which permits consumers to make online payments to merchants** and other individuals using their bank account or credit/debit cards.
- It is available in 202 countries and 25 currencies around the world. PayPal builds on the existing financial infrastructure of the countries in which it operates.
- You establish a PayPal account by specifying a credit, debit, or checking account you wish to have charged or paid when conducting online transactions.
- When you make a payment using PayPal, you e-mail the payment to the merchant's PayPal account.
- PayPal transfers the amount from your credit or checking account to the merchant's bank account.
- The beauty of PayPal is that no personal credit information has to be shared among the users, and the service can be used by individuals to pay one another even in small amounts. However, one issue with PayPal is its relatively high cost.

MOBILE PAYMENT SYSTEMS: YOUR SMARTPHONE WALLET

- The use of mobile devices as payment mechanisms is already well established in Europe and Asia and is now exploding in the United States, where the infrastructure to support mobile payment is finally being put in place.
- Near field communication (NFC) is the primary enabling technology for mobile payment systems.
- **Near field communication (NFC) is a set of short-range wireless** technologies used to share information among devices within about 2 inches of each other (50 mm).
- NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone), and one target device, such as a merchant NFC reader, that can respond to requests from the initiator.
- NFC targets can be very simple forms such as tags, stickers, key fobs, or readers.
- NFC peer-to-peer communication is possible where both devices are powered.

- Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases.
- In September 2014, Apple introduced the iPhone 6, which is equipped with NFC chips designed to work with Apple's mobile payments platform, Apple Pay.
- Building on Apple Passbook and Touch ID biometric fingerprint scanning and encryption that Apple previously introduced in September 2012, Apple Pay is able to be used for mobile payments at the point-of-sale at a physical store as well as online purchases using an iPhone.
- Other competitors in NFC-enabled mobile payments include Android Pay, Samsung Pay, PayPal, and Square. Surveys reveal that about 20%–30% of smartphone users have downloaded mobile wallet apps, but that only about 20% of these adopters have made a payment in the last month using these apps.

SOCIAL/MOBILE PEER-TO-PEER PAYMENT SYSTEMS

- In addition to using a mobile device as a vehicle for e-commerce and as a payment method at physical point-of-sale, another type of mobile payment transaction is becoming increasingly popular: social/mobile peer-to-peer payments.
- Services such as Venmo, Square Cash, Snapcash, the newly refocused Google Wallet, and the new Facebook Messenger Payment service all enable users to send another person money through a mobile application or website, funded by a bank debit card.
- There is no charge for this service.
- Currently, these services are the most popular among Millennials, which is the key demographic driving their growth. Venmo, owned by PayPal, is particularly popular, with its success in part due to its integration with Facebook and its social network newsfeed, which lets users see when friends are paying other friends or paying for products and services.

DIGITAL CASH AND VIRTUAL CURRENCIES

- Although the terms digital cash and virtual currencies are often used synonymously, they actually refer to two separate types of alternative payment systems.
- **Digital cash** typically is based on an algorithm that generates unique authenticated tokens representing cash value that can be used "in the real world." Bitcoin is the best known example of digital cash.
- Bitcoins are encrypted numbers (sometimes referred to as cryptocurrency) that are generated by a complex algorithm using a peer-to-peer network in a process referred to as "mining" that requires extensive computing power.
- Like real currency, Bitcoins have a fluctuating value tied to open-market trading.
- Like cash, Bitcoins are anonymous—they are exchanged via a 34-character alphanumeric address that the user has, and do not require any other identifying information.

- Bitcoins have recently attracted a lot of attention as a potential money laundering tool for cybercriminals and illicit drug markets like Silk Road, and have also been plagued by security issues, with some high-profile heists.
- Nonetheless, there are companies now using Bitcoins as a legitimate alternative payment system.
- **Virtual currencies, on the other hand, typically circulate primarily within an** internal virtual world community, such as Linden Dollars, created by Linden Lab for use in its virtual world, Second Life.
- Virtual currencies are typically used for purchasing virtual goods.

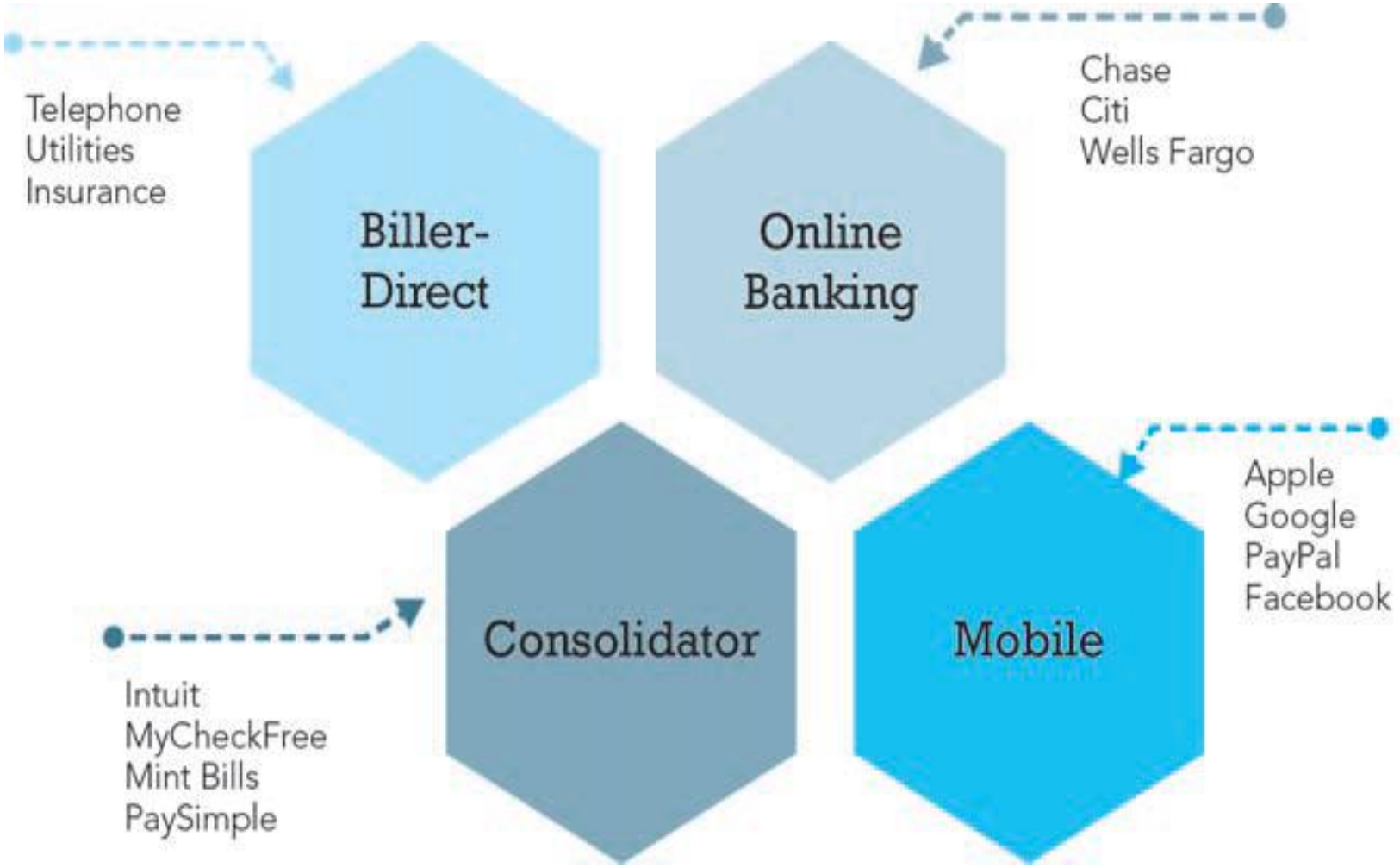
ELECTRONIC BILLING PRESENTMENT AND PAYMENT

- In 2007, for the first time, the number of bill payments made online exceeded the number of physical checks written in the United State.
- In the $19 trillion U.S. economy with a $13.3 trillion consumer sector for goods and services, there are billions of bills to pay.
- According to the U.S. Postal Service, U.S. households received about 21 billion bills in 2015 via the mail.
- No one knows for sure, but some experts believe the life-cycle cost of a paper bill for a business, from point of issuance to point of payment, ranges from $3 to $7.
- This calculation does not include the value of time to consumers, who must open bills, read them, write checks, address envelopes, stamp, and then mailremittances.
- The billing market represents an extraordinary opportunity for using the Internet as an electronic billing and payment system that potentially could greatly reduce both the cost of paying bills and the time consumers spend paying them.
- Estimates vary, but online payments are believed to cost between only 20 to 30 cents to process.

Electronic billing presentment and payment (EBPP) systems

- They are systems that enable the online delivery and payment of monthly bills.
- EBPP services allow consumers to view bills electronically using either their desktop PC or mobile device and pay them through electronic funds transfers from bank or credit card accounts.
- More and more companies are choosing to issue statements and bills electronically, rather than mailing out paper versions, especially for recurring bills such as utilities, insurance, and subscriptions.

MAJOR PLAYERS IN THE EBPP MARKETSPACE



Secure Electronic Transaction (SET) Protocol

- Visa and MasterCard have jointly developed the (SET) Secure Electronic Transaction protocol as a method to secure payment card transactions over open networks.
- SET is being published as an open specification for the industry.
- This specification is available to be applied to any payment service and may be used by software vendors to develop applications.
- Advice and assistance in the development of this specification have been provided by GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa, and VeriSign.

Purpose of Secure Electronic Transaction

- To meet these needs, the SET Secure Electronic Transaction protocol uses cryptography to:

1. provide confidentiality of information,
2. ensure payment integrity, and
3. authenticate both merchants and cardholders.

- This specification will enable greater payment card acceptance, with a level of security that will encourage consumers and businesses to make wide usage of payment card products in this emerging market.

Seven Business Requirements

- SET addresses seven major business requirements:

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers.

Features of the SET specification

- These requirements are addressed by the following features of this specification:

1. Confidentiality of information
2. Integrity of data
3. Cardholder account authentication
4. Merchant authentication
5. Interoperability

- For the sake of clarity, each of these features is described as a distinct component.
- However, these elements do not function independently; all security functions must be implemented.

1. Confidentiality of information

- To facilitate and encourage electronic commerce using payment card products, it will be necessary to assure cardholders that their payment information is safe and can only be accessed by the intended recipient.
- Therefore, cardholder account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals.
- **Online shopping**: In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with few security precautions, if any. However, this account information provides the key elements needed to create counterfeit cards and/or fraudulent transactions.
- **Fraud**: While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high-volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers from a data stream), and the potential for "mischievous fraud" that appears to be characteristic of some hackers.
- **SET's use of message encryption ensures confidentiality of information**

2. Integrity of data

- The specification must guarantee that message content is not altered during the transmission between the originator and the recipient.
- Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. If any component is altered in transit, the transaction will not be processed accurately.
- To eliminate this potential source of fraud and/or error, SET must provide the means to ensure that the contents of each order and payment message received matches the contents of the message sent.
- **SET provides for digital signatures, which ensure the integrity of payment information.**

3. Cardholder account authentication

- Merchants need a way to verify that a cardholder is a legitimate user of a valid branded payment card account number.
- A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing.
- This specification defines the mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.
- **Note**: This specification does not define the process used by a financial institution to determine whether an individual is a legitimate user of an account.
- **SET uses digital signatures and cardholder certificates to ensure the authentication of the cardholder account.**

4. Merchant authentication

- The specification must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards.
- Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.
- **SET provides for the use of digital signatures and merchant certificates to ensure authentication of the merchant**

5. Interoperability

- The specification must be applicable on a variety of hardware and software platforms, and must not include a preference for one over another.
- Any cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard.
- **SET interoperability uses specific protocols and message formats to provide interoperability.**

Participants in SET

Interaction of participants

- SET changes the way that participants in a payment system interact.
- In a face-to-face retail transaction or a mail order transaction, electronic processing begins with the merchant or the Acquirer.
- However, in a SET transaction, the electronic processing begins with the cardholder.

1. Cardholder

- In the electronic commerce environment, consumers and corporate purchasers interact with merchants from personal computers.
- A cardholder uses a payment card that has been issued by an Issuer.
- SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential.

2. Issuer

- An Issuer is a financial institution that establishes an account for a cardholder and issues the payment card.
- The Issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.

3. Merchant

- A merchant offers goods for sale or provides services in exchange for payment.
- With SET, the merchant can offer its cardholders secure electronic interactions.
- A merchant that accepts payment cards must have a relationship with an Acquirer.

4. Acquirer

- An Acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

5. Payment gateway

- Payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.

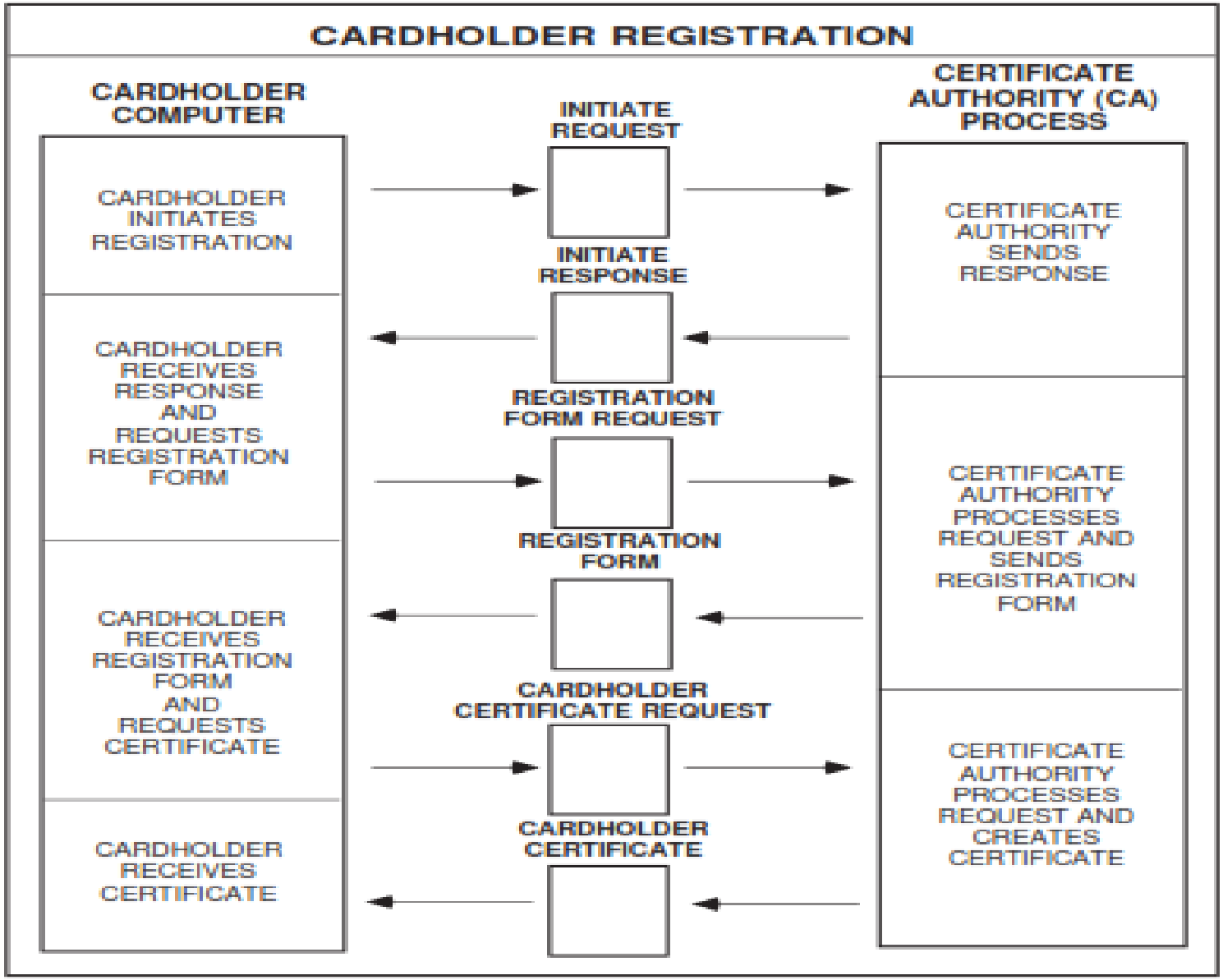
6. Brand

- Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks to interconnect the financial institutions.
- Other brands are owned by financial services companies that advertise the brand, and establish and enforce rules for use and acceptance of their payment cards.
- These brands combine the roles of Issuer and Acquirer in interactions with cardholders and merchants.

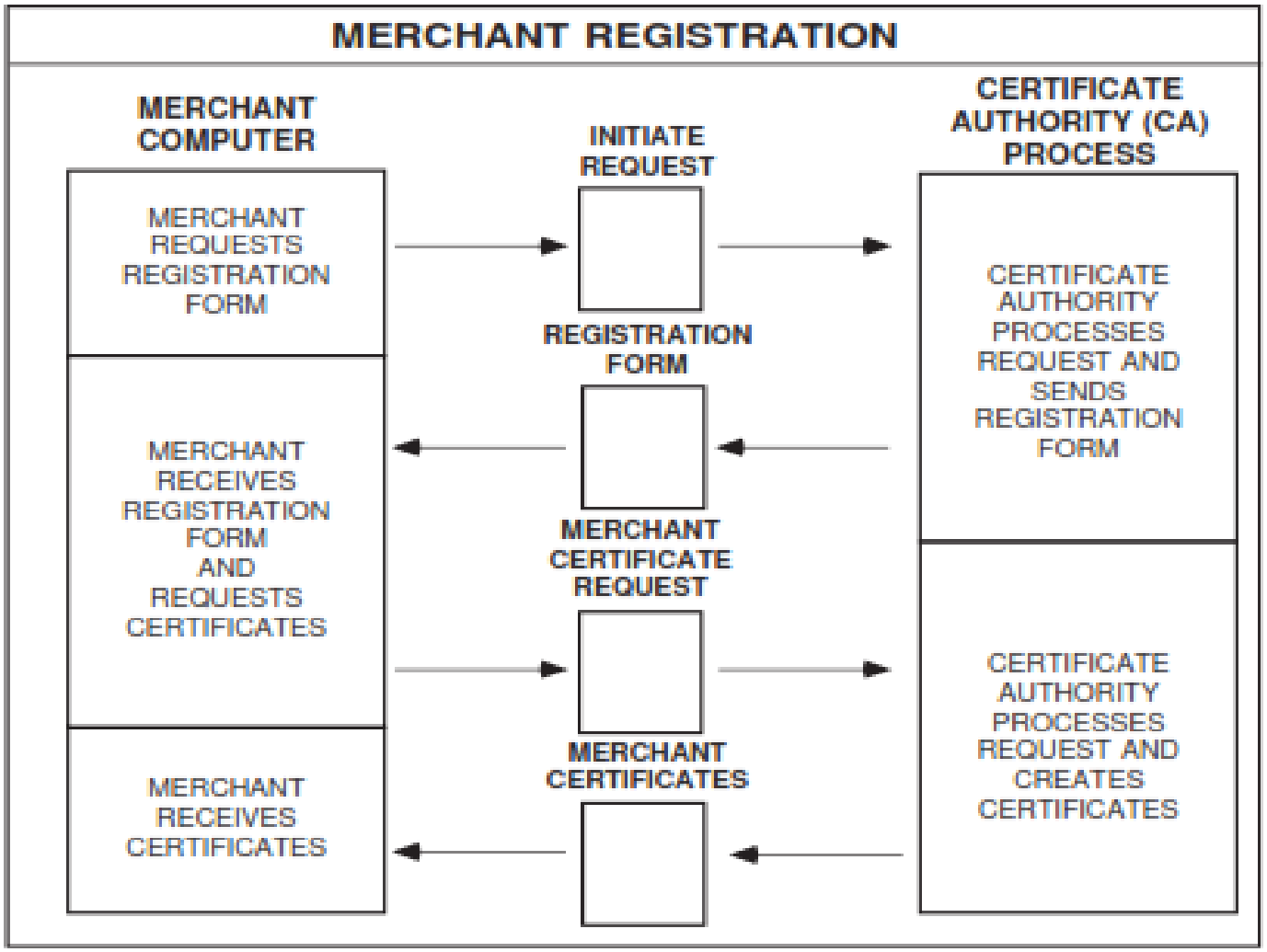
7. Third parties

- Issuers and Acquirers sometimes choose to assign the processing of payment card transactions to third-party processors.
- This document does not distinguish between the financial institution and the processor of the transactions.

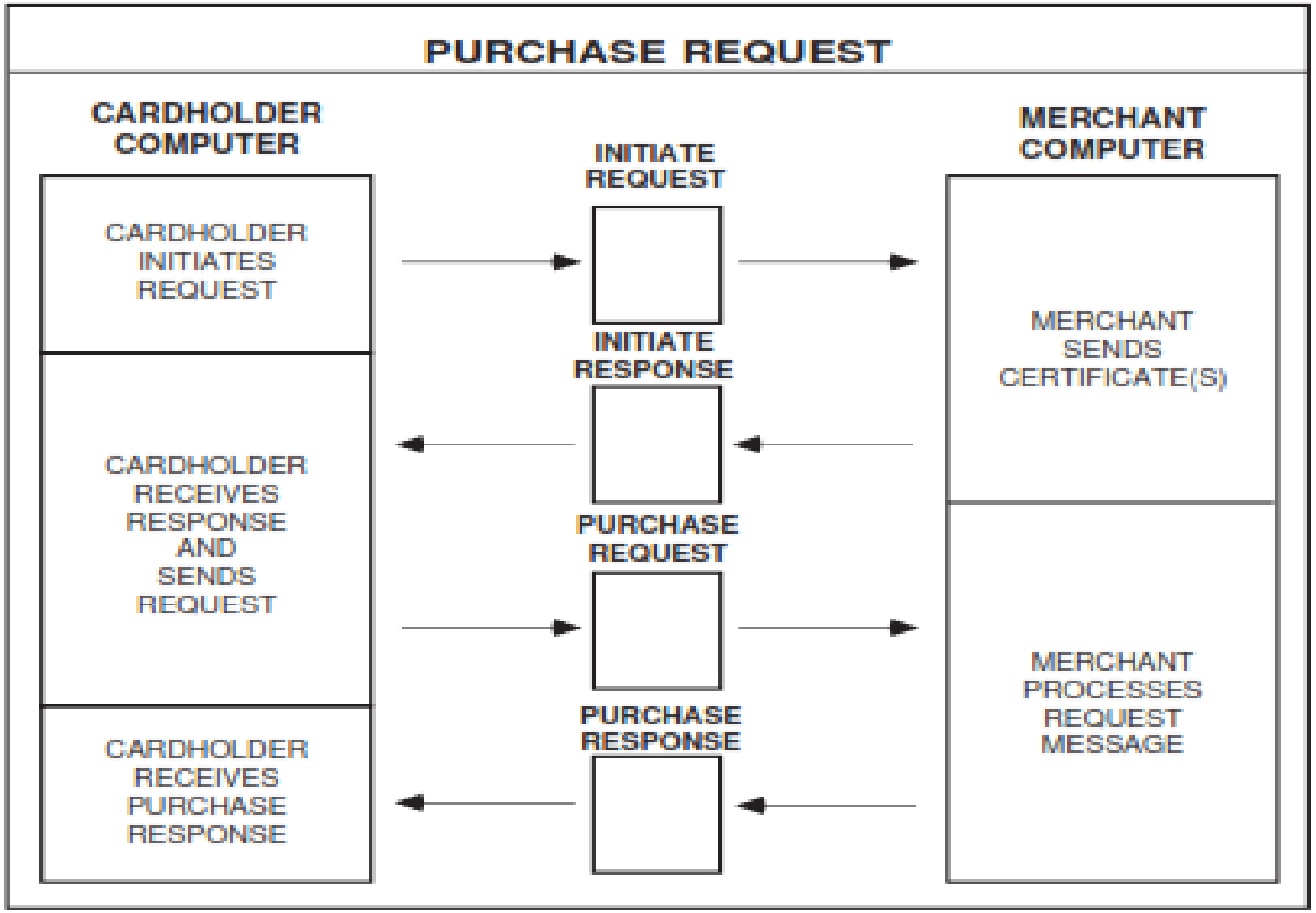
Cardholder Registration



Merchant Registration



Purchase Request



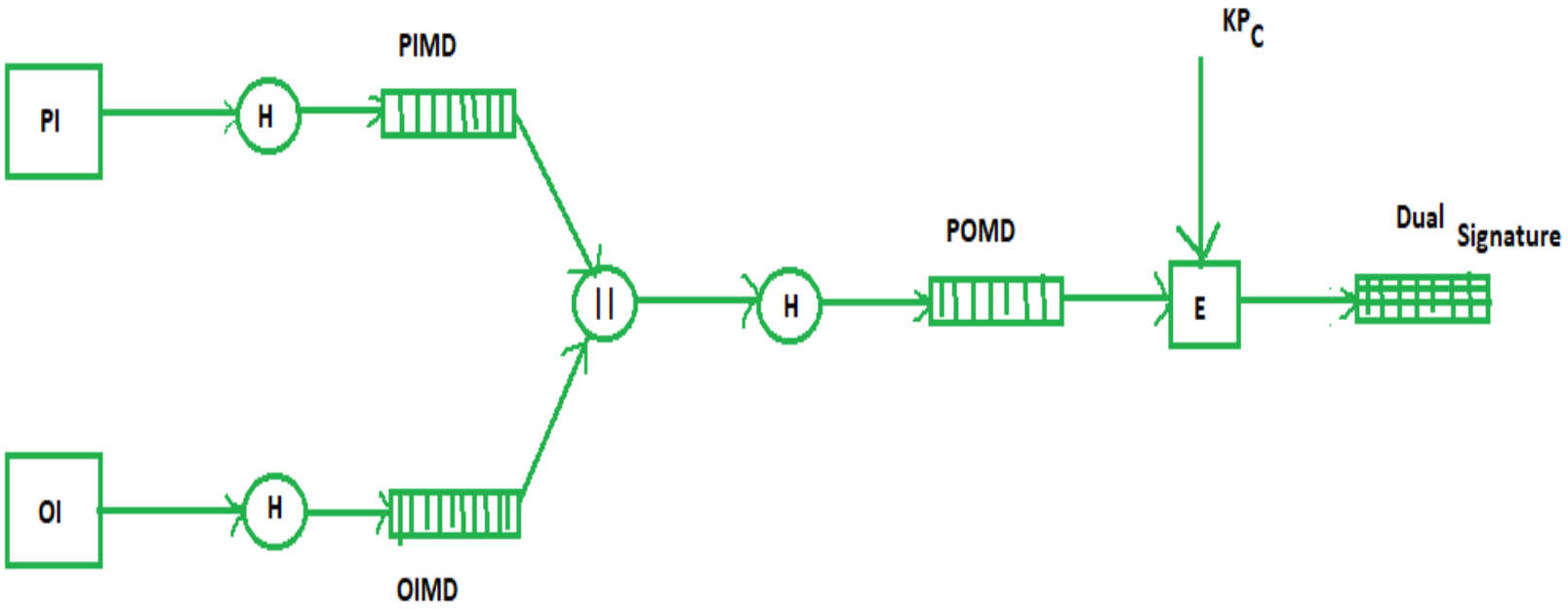
Dual Signature

- The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

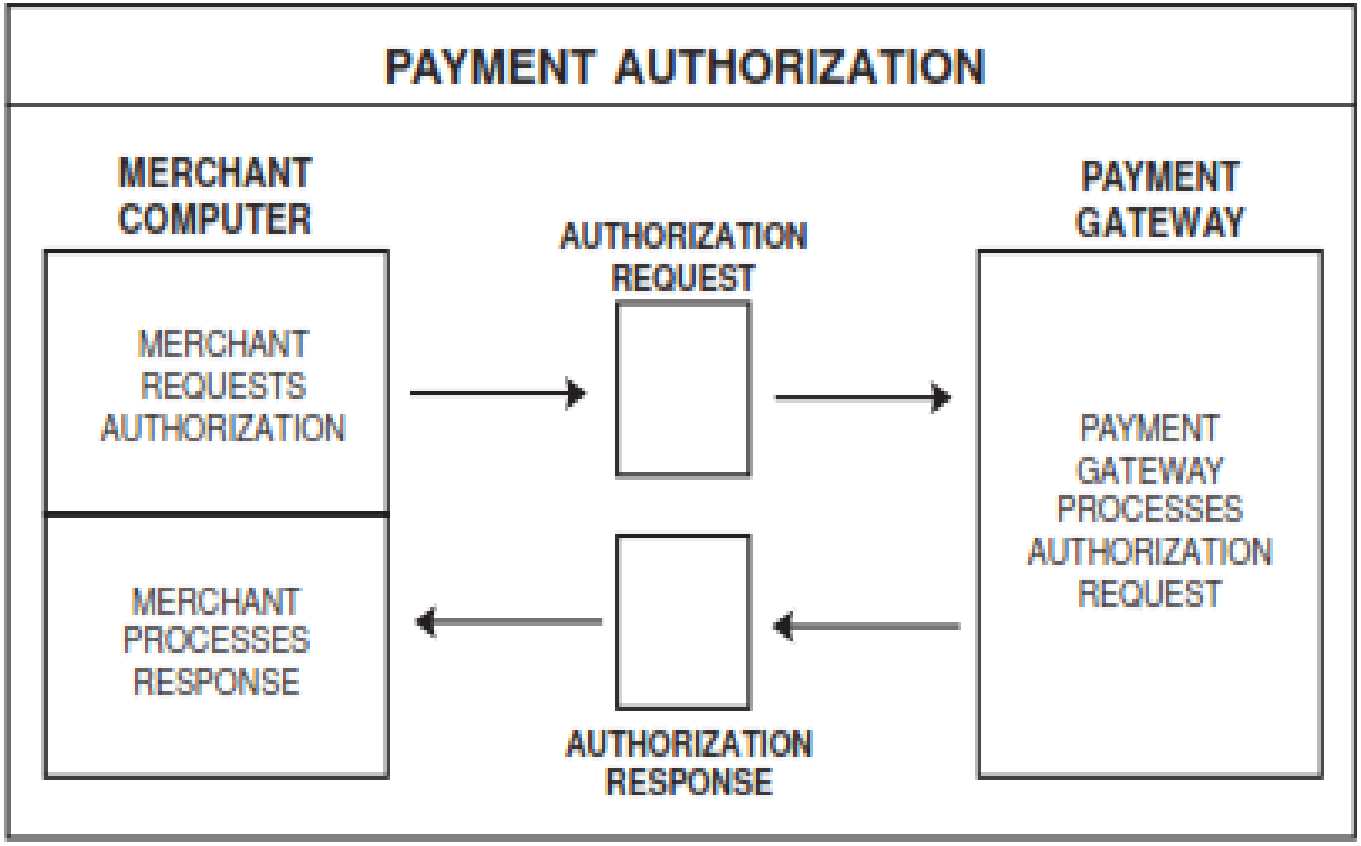
1. **Order Information (OI) for merchant**
2. **Payment Information (PI) for bank**

- You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible.
- Here is the generation of dual signature:

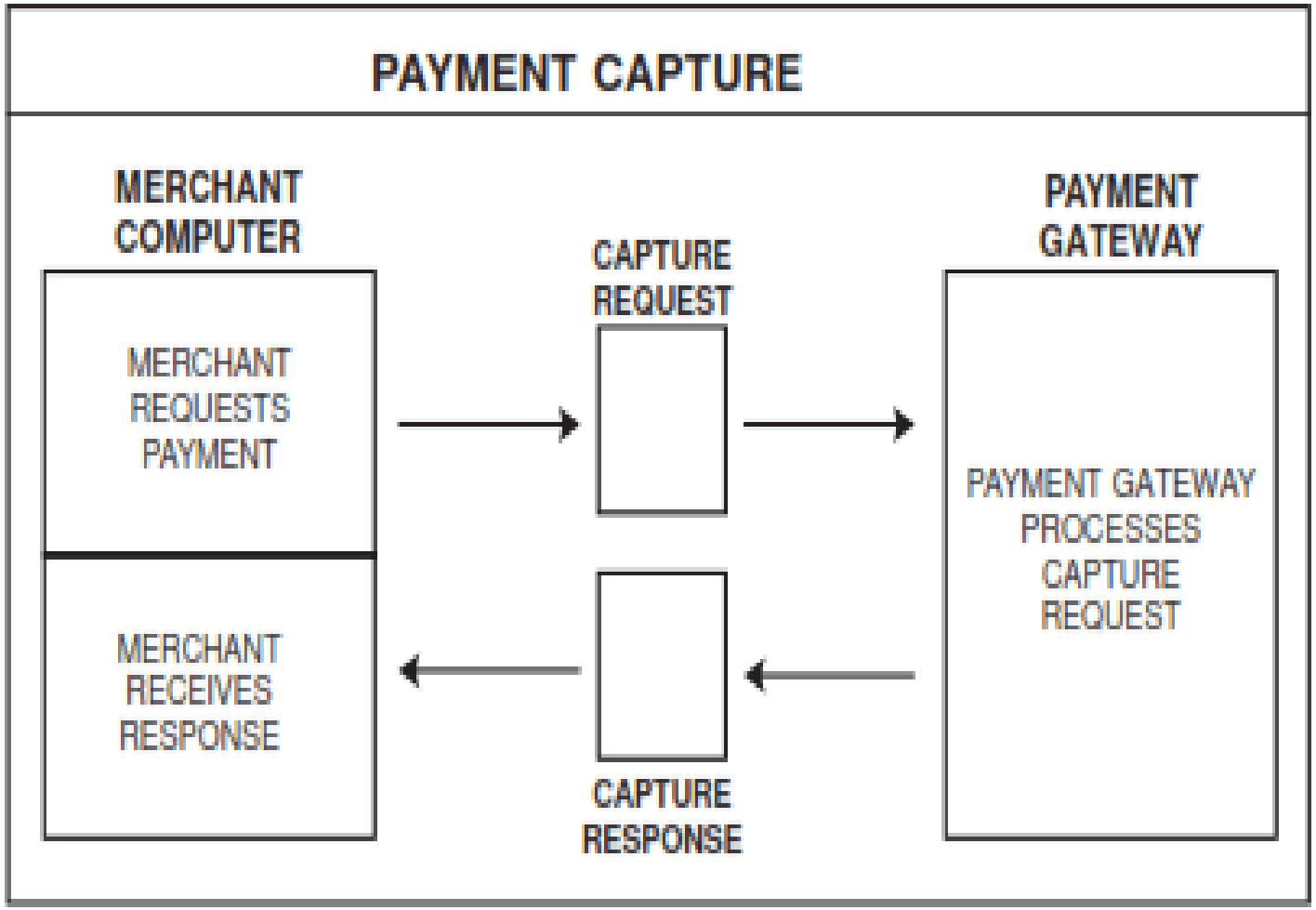
PI stands for payment information
OI stands for order information
PIMD stands for Payment Information Message Digest
OIMD stands for Order Information Message Digest
POMD stands for Payment Order Message Digest
H stands for Hashing, **E** stands for public key encryption KPc is customer's private key
|| stands for append operation Dual signature,
DS= E(KPc, [H(H(PI)||H(OI))])



Payment Authorization



Payment Capture



Home Assignment: 3

1. Status of E-Payment Systems in Nepal
2. Case Studies of Global and Local Payment Systems