The University Of Queensland AUSTRALIA | CREATE CHANGE

Business Information Security

Week 10:

- Online payment discussion – how is it done!
- PCI DSS – Payment Card Industry Data Security Standard

Dr Alex Pudmenzky

Semester 2, 2024

October 2024: Cyber Security Awareness Month

https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/2024-cyber-security-awareness-month#

Live hacking demonstration with Rachel Tobac

How I would hack you and how to stop me: live hacking demonstration with Rachel Tobac
Date: Thursday 24 October 2024
Time: Arrive 11.45am for a 12-1pm event, followed by refreshments
Venue: 49-200 Advanced Engineering Building, GHD Auditorium, St Lucia campus
This event has limited seating and registration is required.
If you are unable to attend in person, email cyberculture@uq.edu.au for other arrangements.

Have you ever wondered how cyber criminals hack people and if you could be their next victim?
Rachel Tobac will demonstrate how easily we can fall victim to cyber crime by giving a live hacking demonstration on a willing UQ staff volunteer. It only takes one email, a 30 second call or one social media DM for her to hack you and gain access to your money, data and systems. Rachel will break down recent cyber attacks and demonstrate how to defend against the latest hacking methods during this interactive and engaging presentation.

Presenter
Rachel Tobac is an ethical hacker and CEO of SocialProof Security where she uses social engineering to provide training and pen testing for individuals and companies to keep their data safe. Rachel has shared her real life social engineering stories with Last Week Tonight with John Oliver, The New York Times, CNN, NBC Nightly News and many more.

Watch live hack: https://www.youtube.com/watch?v=LYilP-1TwMg

How to spoof a phone number

WARNING:

Spoofing a phone number in Australia is generally **illegal** if it is done for fraudulent or malicious purposes, such as carrying out scams. Legitimate uses, like displaying a different number for business purposes, are allowed as long as they are not intended to deceive or harm.

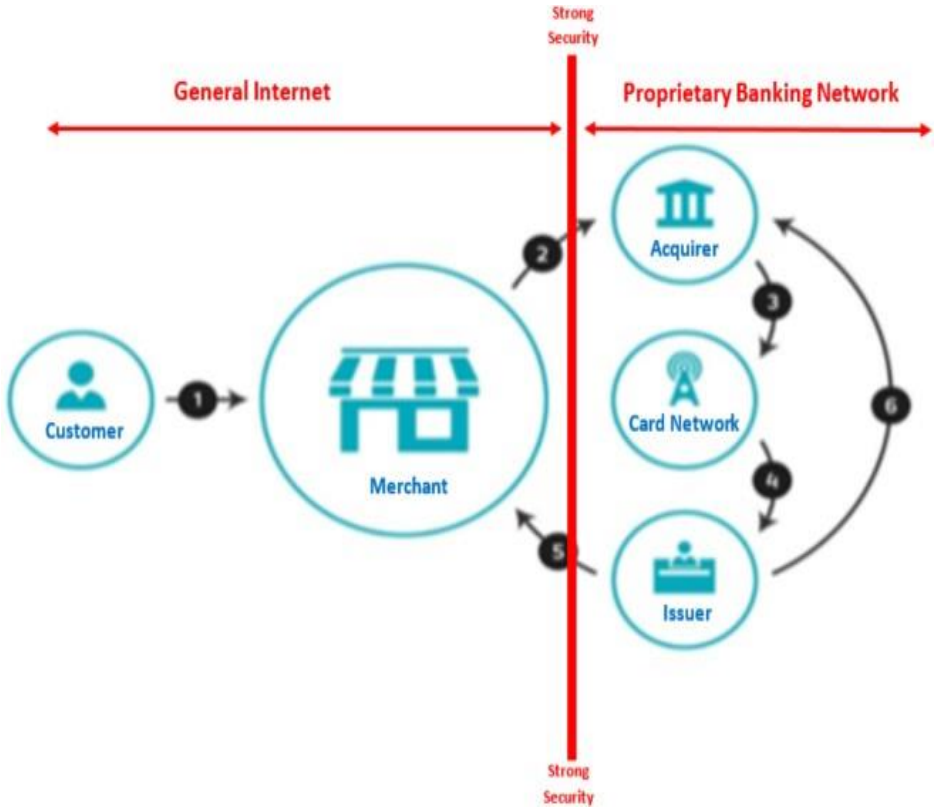
Penalties for engaging in illegal phone number spoofing can be severe. Telcos face penalties of up to **$250,000** for breaching the Australian Communications and Media Authority (ACMA) directions to comply with anti-scam regulations. Additionally, individuals involved in fraudulent activities using spoofed numbers can face legal consequences, including **fines and potential criminal charges**.

https://www.spoofcard.com/

https://smartphones.gadgethacks.com/how-to/make-spoofed-calls-using-any-phone-number-you-want-right-from-your-smartphone-0242383/

PCI DSS* – Firstly - Credit/Debit Card Payments

We can categorize credit card payments as those were the card is present at the transaction and those were the card is not present at the transaction.

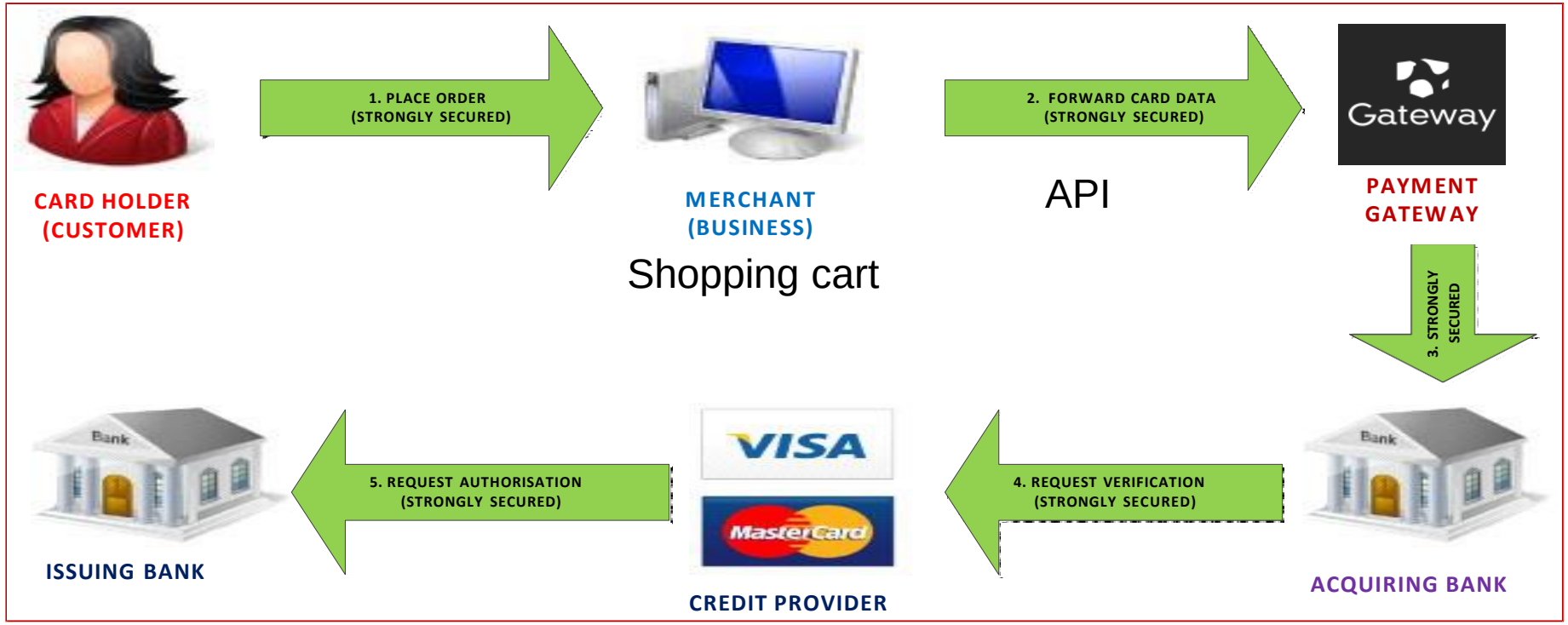


Acquirer – merchant bank
Issuer – a bank, credit union, saving, loan association, or retailer that provides a credit line or a debit card to a consumer or business

1. Customer pays with card
2. Payment is authenticated – merchant captures customer's account info and sends it to acquirer
3. Transaction is submitted – merchant acquirer asks the card brand to get an authorization from the customer's issuing bank
4. Authorization is requested – card brand submits the transaction to the issuer for authorization
5. Authorization response – issuing bank authorizes the transaction and routs the response back to the merchant
6. Merchant payment – issuing bank routes the payment to the merchant's acquirer for deposit into the merchant's account

*Payment Card Industry - Data Security Standard (PCI- DSS)

E-business: The Online Transaction (1)



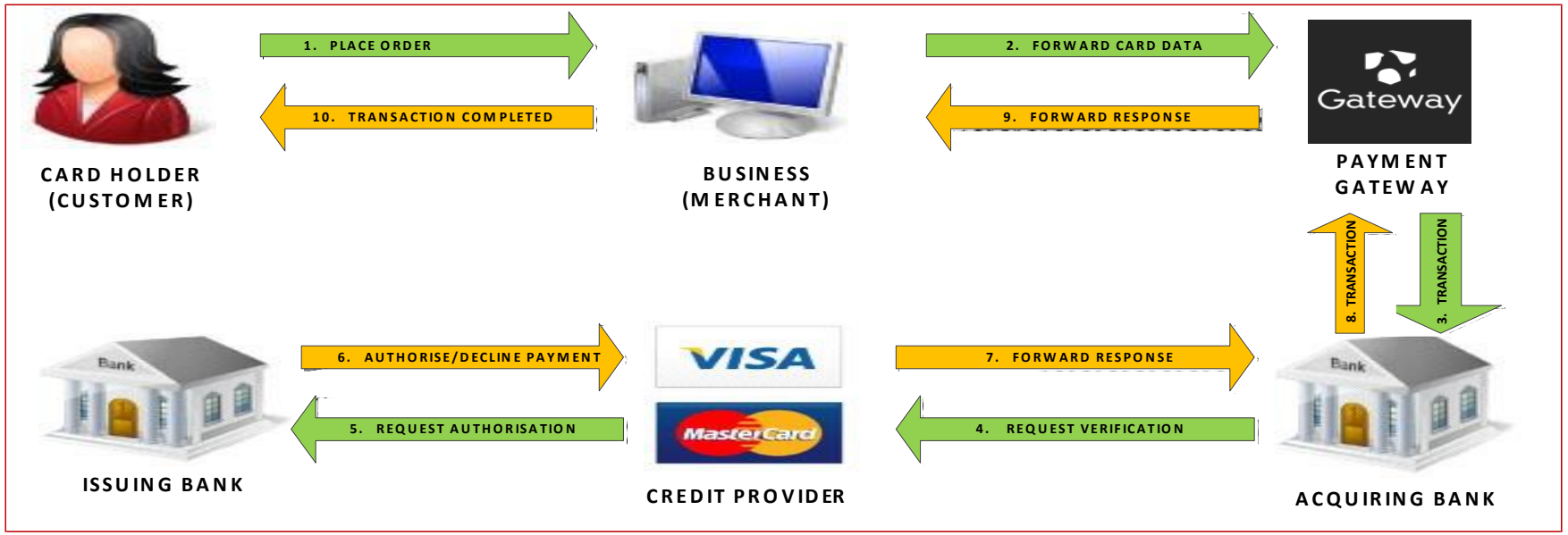
Bank of customer (check)

Bank of shop

1. **The CARD HOLDER initiates the ONLINE PURCHASE (e.g. via a 'shopping cart'). The ACCOUNT DETAILS and PRODUCT DETAILS are passed VERY SECURELY to the MERCHANT (i.e. web site)**
2. **The MERCHANT then sends all these details very securely to the PAYMENT GATEWAY (the entrance to the FINANCIAL NETWORK)**
3. **The PAYMENT GATEWAY sends the secured transaction to the ACQUIRING BANK.**
4. **The ACQUIRING BANK sends the secured transaction to the CREDIT PROVIDER.**
5. **The CREDIT PROVIDER sends the secured transaction to the ISSUING BANK which performs debit/credit checks and issues APPROVAL/REJECTION**

E-business: The Online Transaction (2)

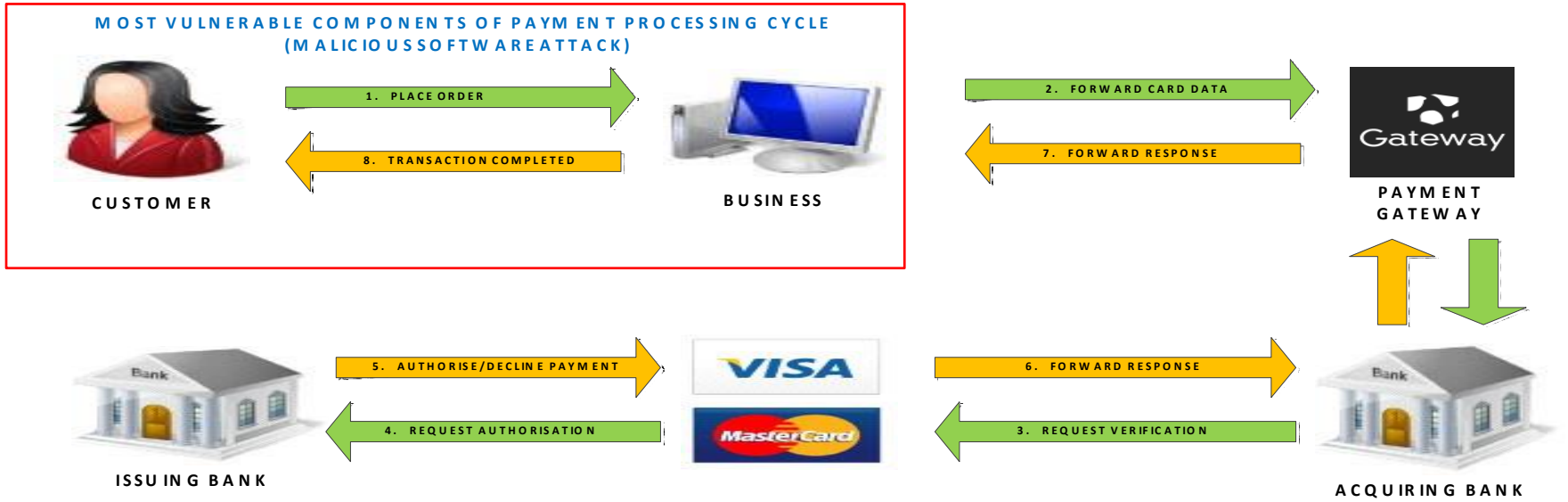
Bank of customer (check)



Bank of shop

- The ISSUING BANK – sends back a response to CREDIT PROVIIDER, and then to the ACQUIRING BANK with a response code (approved/denied). Response code also defines the reason for failure (e.g. insufficient funds).
- The ISSUING BANK holds an authorization associated with that merchant and consumer for the approved amount
- ACQUIRING BANK forwards the authorization response to the PAYMENT GATEWAY, which forwards it to the BUSINESS/MERCHANT - this is known as the Authorization or "Auth". *Entire process typically takes 1 – 3 seconds*
- **MERCHANT then fulfils the order**. The process is repeated but this time to "Clear" the authorization by consummating the transaction.
- The MERCHANT submits all approved transactions in a "batch" to their ACQUIRING BANK.
- *The entire process from authorization to settlement to funding typically takes 3 days.*

E-business: The Online Transaction (3)



- Easily the most vulnerable entities within this online transaction cycle are the CARD HOLDER/CUSTOMER machine AND the BUSINESS WEB SITE (web server and database server).
- The NETWORK LINKS are very secure due to the SECURITY COMMUNICATION PROTOCOL used.
- The FINANCIAL NETWORK entities are very secure (not perfectly) – this is primarily because of a strong, well resourced focus on SECURITY POLICY and IMPLEMENTATION OF APPROPRIATE CONTROLS
- The CUSTOMER machine and the BUSINESS WEB SITE are vulnerable to a variety of security attacks – but mainly to MALWARE (malicious software).
  - PC's / LAPTOPS / TABLETS (and mobile/smart phones) are still not well designed for security

Merchant Account Fees

- **Authorization Fee**
  - Really an 'authorization request fee – is charged each time a transaction is sent to the card-issuing bank to be authorized – applies regardless of whether the request is approved
  - NOT the same as Transaction fee
- **Transaction Fee**
  - Is charged when you accept your authorization – only applies to an authorization that is accepted without error
- **Statement Fee**
  - Monthly fee associated with the monthly statement that is sent to the merchant at the end of each month processing cycle
- **Monthly Minimum Fee**
  - To ensure that merchants pay a minimum amount in fees each month to cover costs from the provider to maintain the account
- **Batch Fee**
  - AKA a batch header fee, when the merchant sends their completed transactions for the day to their acquiring bank for payment – important to close a batch every 24 hours or a higher rate is assessed by Visa / MasterCard / Discover
- **Customer Service Fee**
  - AKA a maintenance fee, merchant support fee, customer support fee, service fee
- **Annual Fee**
  - Levied by some providers – levied quarterly in most cases
- **Early Termination Fee**
  - If the merchant ends the contract before the end of the contract term

The business contributes most of that money!

Merchant Account Fees (Continued)

Chargeback Fee

- **Exists for consumer protection**
- Originated in U.S. when consumers were afforded 'reversal rights' in legislation – **now extended globally.**
- **A consumer initiates a chargeback – contacts issuing bank and files a substantiated complaint regarding one or more debit items on statement**
- Reversal of funds aims to:
  - Provide incentive to merchants for quality products, helpful customer service, and timely refunds as appropriate
  - Provide a means to counter unauthorized transfers due to identity theft.
- Chargeback rules should always be available publicly for consumers
- **Chargeback is the largest risk that is presented to banks and providers** – not to be confused with a refund
- In Visa, Discover, and MasterCard rules, the merchant's processing bank is 100% responsible for all the transactions that the merchant performs. Leaves the provider open to large potential losses if the merchant operates in an illegal or risky manner
- Providers pass this cost on to the merchant – if the merchant can pay
- If a chargeback occurs, merchant may be assessed a fee by their acquiring bank
- Currently both Visa and MasterCard require all merchants to maintain no more than 1% of dollar volume processed to be chargebacks – if above: (high) fines to the merchant's processing bank – ultimately passed onto merchant

PCI DSS – Overview #1

- **Rationale**: An information security standard – targeting merchants and service provides – protects credit/debit card data during storage, transmission, processing – not aimed directly at customers
- **Origins:**
  - *2001* – Visa mandated adoption of CISP (a security program) – 12 security requirements
  - Other brands developed their own:
    - American Express – Data Security Operating Policies (DSOP)
    - Discover – Information Security Compliance (DISC)
    - MasterCard – Site Data Protection Program (SDP)
    - JCP – Data Security Program (DSP)
  - *2004* – Visa & MasterCard merged their security programs into a single standard – PCI DSS.
  - *2006* – Visa, MasterCard, Am Express, Discover Financial Services & JCB International formed the **PCI Security Standards Council** to manage the evolution of the PCI DSS.
  - *2022* – most recent version PCI-DSS 4.0
- The PCI-DSS is not law and compliance enforcement and non-compliance penalties are set by an individual brand through contractual penalties or sanctions. E.g. Visa & MasterCard transactions are enforced by the merchant's acquirer. American Express deals directly with its merchants for compliance.

PCI DSS – Overview #2

Capstone: The PCI-DSS forms a capstone standard:

- PCI-DSS is the top-level standard.
- PCI PA-DSS (Payment Application DSS) is for software developers/integrators of applications that store, process or transmit cardholder data as part of the authorization of settlement.
- PCI PTS (PIN Transaction Security) applies to manufacturers of personal identification number (PIN) entry terminals used for payment card financial transactions.
- PCI Point-to-Point Encryption Standard (P2PE). As the payment card is swiped through a merchant's card reading device (the point of interaction (POI) device), the data is immediately encrypted. The encrypted data is then sent immediately to the payment processor (i.e. the banking network). The keys for encryption/decryption are never available to the merchant making card data entirely invisible to the retailer.
- 2 other standards:
  - PCI Card Production Logical Security Requirements and Physical Security Requirements (card manufacturing, chip personalization, PIN distribution, etc.
  - PCI Token Service Provider Security Requirements

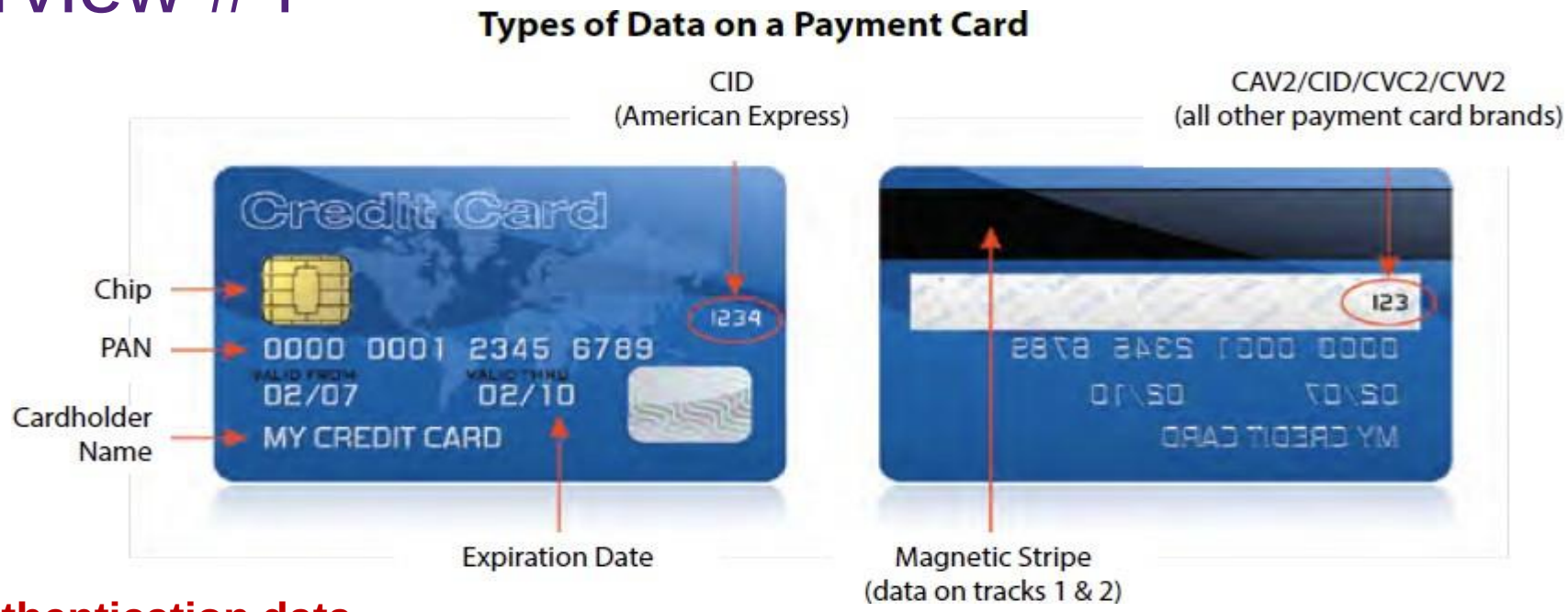
PCI DSS – Overview #3

- **High level overview**
  - PCI DSS applies to ***all*** entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. PCI DSS applies to ***all*** other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	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.	Protect all systems against malware 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.	Identify and authenticate access to system components
	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 all personnel

PCI DSS – Overview #4



Cardholder data and sensitive authentication data

- **PCI DSS goal** – to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted.
- **PAN** – the primary account number printed on the front of the card
- Merchants, service providers, and other entities involved in payment card processing **must never store sensitive authentication data after authorization**. This includes:
  - The 3 or 4 digit security code printed on the front or back of the card
  - The data stored on the card's magnetic stripe or chip (the "Full Track Data")
  - The personal identification numbers (PIN) entered by the cardholder

PCI DSS – Overview #5

Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

- The primary account number (PAN) is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements.
- Organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party as per the applicable PCI DSS requirements
- Cardholder data environment is that vital area of the business hardware, software, network links and people that are involved in the processing, storage or transmission of cardholder data.

PCI DSS – Overview #6

Guidelines for Cardholder Data Elements:

PCI DSS Requirement 3 "Protect stored cardholder data"

	Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data[1]	Full Track Data[2]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID[3]	No	Cannot store per Requirement 3.2
	PIN/PIN Block[4]	No	Cannot store per Requirement 3.2

1 Sensitive authentication data must not be stored after authorization (even if encrypted)
2 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.
3 The three- or four-digit value printed on the front or back of a payment card
4 Personal Identification Number entered by cardholder during a transaction, and/or encrypted PIN block present within the transaction message

PCI DSS – **C**ardholder **D**ata **E**nvironment (p.10 PCI DSS v3.2.1)

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

- **Systems** that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors ***(Beyond our scope)***
- **Network components** including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- **Server types** including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- **Applications** including all purchased and custom applications, including internal and external (for example, Internet) applications.
- **Any other component** or device located within or connected to the CDE.

PCI DSS – **CDE Scope and Network Segmentation**

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

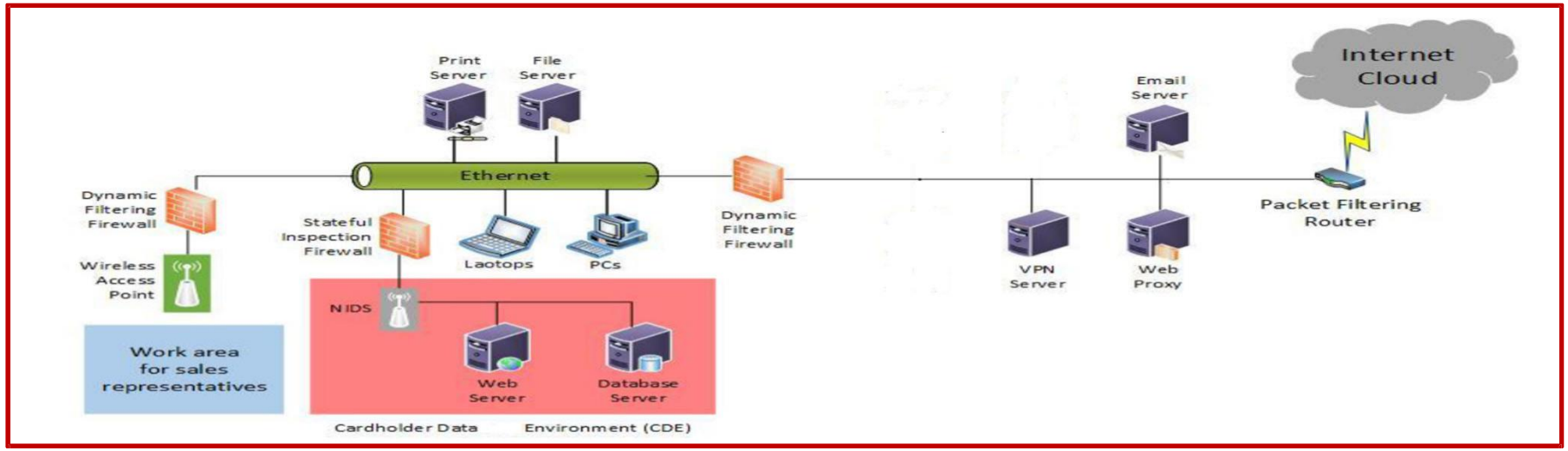
- *The scope of the PCI DSS assessment*
- *The cost of the PCI DSS assessment*
- *The cost and difficulty of implementing and maintaining PCI DSS controls*
- *The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)*

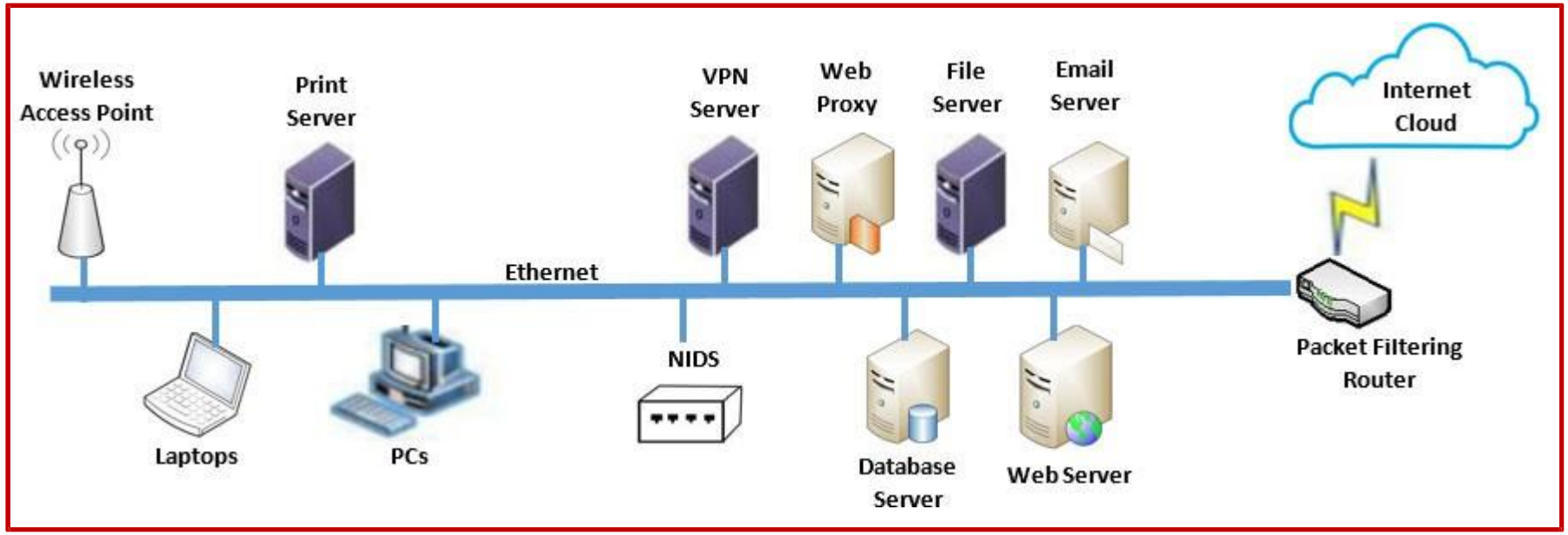
*Without adequate network segmentation (sometimes called a "flat network") **the entire network is in scope of the PCI DSS assessment***

	Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data[1]	Full Track Data[2]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID[3]	No	Cannot store per Requirement 3.2
	PIN/PIN Block[4]	No	Cannot store per Requirement 3.2

1 Sensitive authentication data must not be stored after authorization (even if encrypted)
2 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.
3 The three- or four-digit value printed on the front or back of a payment card
4 Personal Identification Number entered by cardholder during a transaction, and/or encrypted PIN block present within the transaction message

PCI DSS – **CDE Scope - Network Segmentation vs "Flat Network"**





PCI DSS – **a 'typical' scoping exercise**

(p.9 Guidance-PCI-DSS-Scoping-and-Segmentation_v1-1.pdf)

Activity	Description
Identify how and where the organization receives CHD.	1. Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer.
Locate and document where account data is stored, processed, and transmitted.	2. Document all CHD flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE[7].
Identify all other system components, processes, and personnel that are in scope.	3. Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These people, processes, and technologies are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD.
Implement controls to minimize scope to necessary components, processes, and personnel.	4. Implement controls to limit connectivity between CDE and other in-scope systems to only that which is necessary. 5. Implement controls to segment the CDE from people, processes, and technologies that do not need to interact with or influence the CDE.
Implement all applicable PCI DSS requirements.	6. Identify and implement PCI DSS requirements as applicable to the in-scope system components, processes, and personnel.
Maintain and monitor.	7. Implement processes to ensure PCI DSS controls remain effective day after day. 8. Ensure the people, processes, and technologies included in scope are accurately identified when changes are made.

PCI DSS – E-commerce implementations

(PCI SSC reference: "best_practices-securing_ecommerce.pdf"

Payment Service Provider (PSP): A PSP offers a service that directly facilitates e-commerce transactions online via its relationship with acquiring member banks of payment card brands. This category includes online payment processors, payment "gateway" service providers, virtual terminal services, and certain e-wallet or prepaid services that also process credit card payment for non-account holders at the point of sale.

Common e-commerce implementations:

1. Wholly outsourced e-commerce implementations.
2. Shared-management (merchant & PSP)
   - URL redirection to a PSP
   - An Inline Frame (or "iFrame" – embedding a payment form hosted by a third party within the merchant's web page(s)
3. Merchant-managed e-commerce implementation (commercial shopping cart/payment application fully managed by the merchant)

PCI DSS – (1) Wholly outsourced e-commerce solutions

(PCI SSC reference: "best_practices-securing_ecommerce.pdf" – page 19

- Many e-commerce solutions exist that provide most or the entire merchant's online shopping functionality and experience. These solutions provide more than just transaction processing capability, often including customer-facing features such as product search, cart capability, checkout, and account management; and back-office features such as product management, customer relationship management, order management, and appearance customizations.
- A hosted shopping cart is an e-commerce system that is hosted entirely on the service provider's technological infrastructure. The e-commerce is not seamlessly integrated into the merchant's website and the consumer is often directed off-site to select product and complete checkout.

MERCHANT IMPACT: The use of such a solution can alleviate many but not all of the merchant's PCI DSS responsibilities. All merchants have a responsibility to implement policies and procedures that govern safe handling of cardholder data even if they never expect to encounter credit cards. Furthermore, it is the responsibility of the merchant to vet the service provider and monitor its compliance to PCI DSS. **Number of questions under PCI-DSS: 22**.

PCI DSS – (2) URL redirected e-commerce solutions

(PCI SSC reference: "best_practices-securing_ecommerce.pdf" – page 19

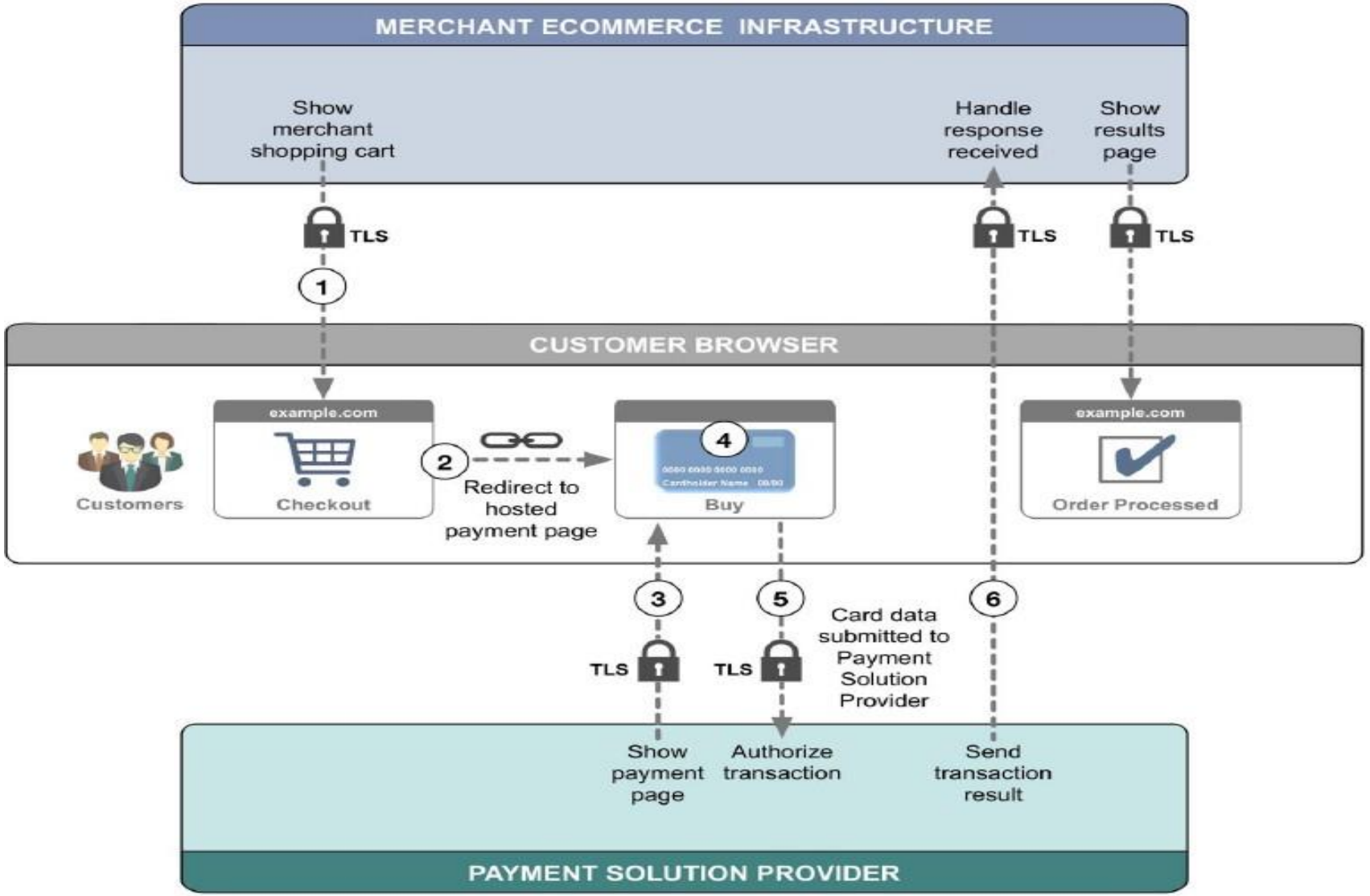
In the URL redirection model, the cardholder is **redirected from the merchant's website to a third-party page**. The cardholder then enters their account data into a payment page hosted by the third-party payment service provider (PSP). That is, customers of the merchant are sent to a PSP's web pages. This is generally noticeable to the customer as the merchant's website URL— e.g., **http://www.merchant.example.com** — changes to that of the PSP—e.g., **https://www.psp.example.com**

MERCHANT IMPACT: As account data is not collected, stored, processed, or transmitted by the merchant's system, fewer systems need security controls - used by small and medium business organizations with lower-than-average cardholder data volume.

This e-commerce option provides an easier way for merchants to provide security for cardholder data, as most of the cardholder data security is performed by the PSP. It is strongly recommended that a merchant ensure the PSP is validated as a PCI DSS compliant service provider. **Number of questions under PCI-DSS - as few as: 22**

Let's conceptualize this 'redirection' strategy

PCI DSS – (2a) URL redirected e-commerce solutions



1. Merchant website sends a redirect command to the customer's browser.
2. The customer's browser then requests a payment form from the PSP.
3. The PSP creates the payment form and sends to the customer's browser.
4. The customer's browser displays the PSP's payment form.
5. The customer enters account data and sends to the PSP.
6. The PSP receives the account data and sends it to the payment system for authorization – PSP sends the result ('approved' or otherwise) to the merchant – merchant advises customer.

PCI DSS – (2b) Inline Frame (iFrame) e-commerce solutions

(PCI SSC reference: "best_practices-securing_ecommerce.pdf" – page 10 – 13 inclusive)

What is an iFrame?

An iFrame (or *Inline Frame*) is a method of seamlessly embedding a web page within another web page — the iFrame becomes a frame for displaying another web page.

- **Security** - The iFrame isolates the content of the embedded frame from the parent web page, thus ensuring that information is not accessible or cannot be manipulated through various exploits by malicious individuals.

In e-commerce payments, the pages delivered during the checkout process would be supplied by the merchant's website, with an embedded iFrame supplied by the PSP within that process. The PSP's iFrame receives all cardholder data entered by the customer.

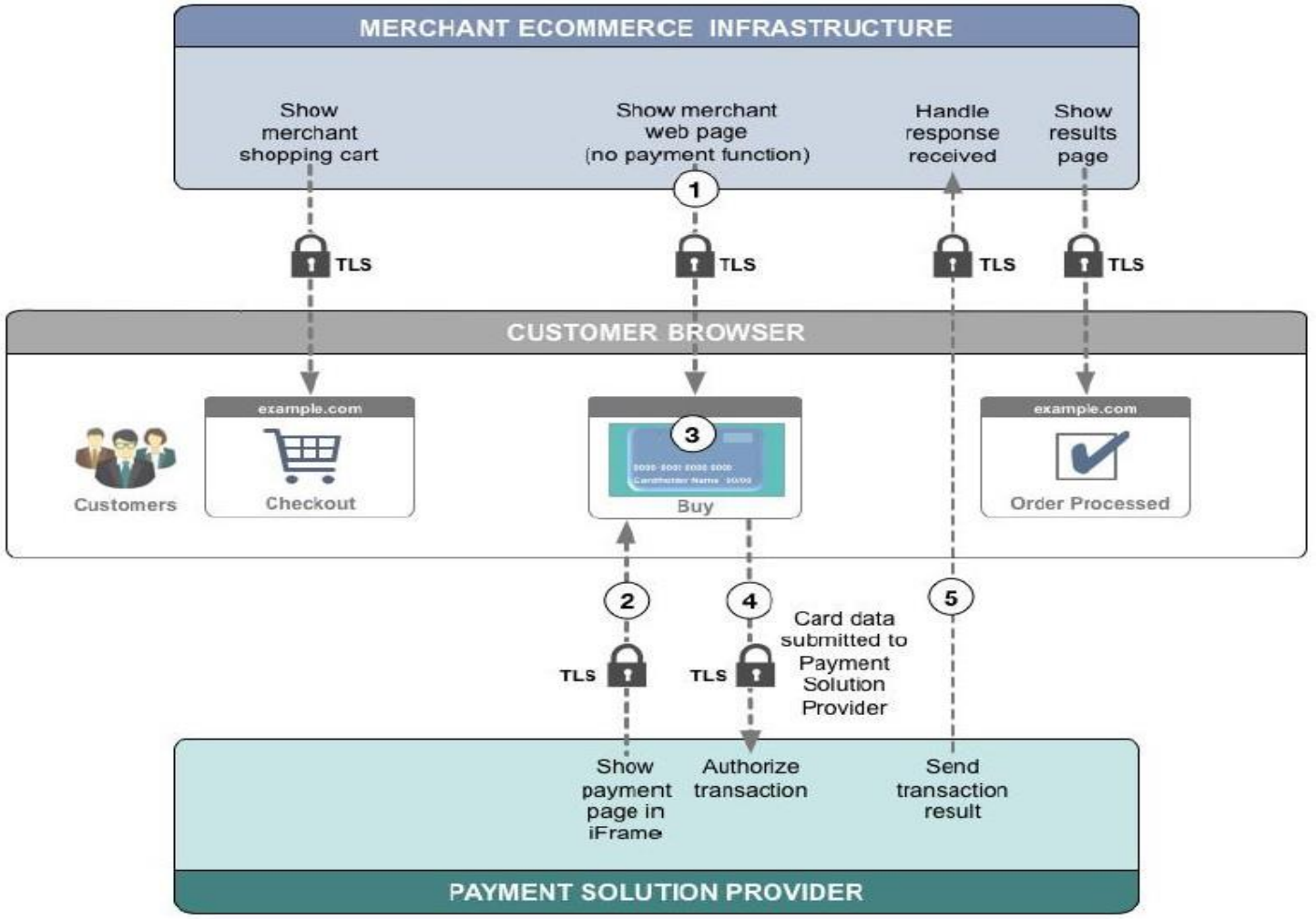
MERCHANT IMPACT:

Payment card data is not collected, stored, processed, or transmitted by the merchant, so there are fewer systems that need security controls and lower risk of the merchant's systems being compromised. This e-commerce option provides an easier way for merchants to provide security for cardholder data as most of the cardholder data security is performed by the PSP.

Number of questions under - as few as: 22

Let's conceptualize this 'iFrame' strategy

PCI DSS – (2b) Inline Frame (iFrame) e-commerce solutions



1. The merchant website creates an iFrame within the current webpage. The customer's browser requests the payment form from the PSP.
2. The PSP creates a payment form and sends to the customer's browser within the iFrame.
3. The customer's browser displays the payment form within the iFrame located on the merchant page.
4. The customer enters their payment details into the iFrame containing the PSP's payment form.
5. The PSP receives the account data and sends it to the payment system for authorization. PSP advises merchant, merchant advises customer.

PCI DSS – (3) Merchant managed e-commerce implementation

(PCI SSC reference: "best_practices-securing_ecommerce.pdf" – page 17 – 19 inclusive)

This approach is via an Application Programming Interface (API) – it principally for 'big-business'. In this context, an application-programming interface (API) is a method of system-to-system data transmission in which the merchant principally controls the progress of the payment transaction.

Customer cardholder data is sent from the customer browser back to the merchant website before being sent to the PSP. The payment page and form are hosted and supplied by the merchant website with all cardholder data processed by the merchant web server (and possibly other system components) before being sent to the PSP.

MERCHANT IMPACT:

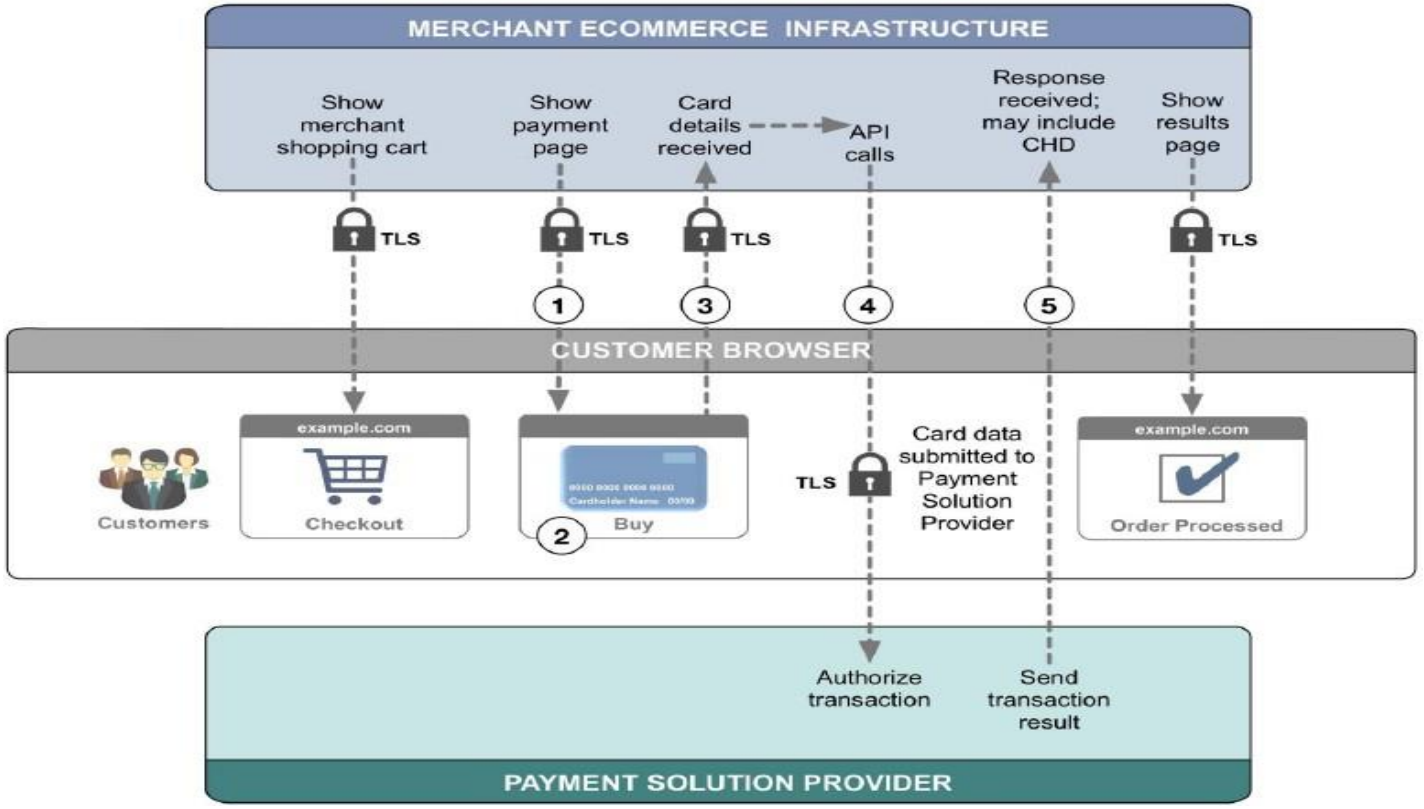
This architecture carries a high risk for merchants as their systems will receive and transmit, and may also store and process, cardholder data.

Hackers target websites using this payment method because there is a greater chance of larger amounts of valuable cardholder data being available, and the attack can be easier due to varying levels of security controls among merchants.

Due to the higher risk of compromise to merchant systems, the level of security responsibly for the merchant is high.
Number of questions under PCI-DSS - approximately: 250

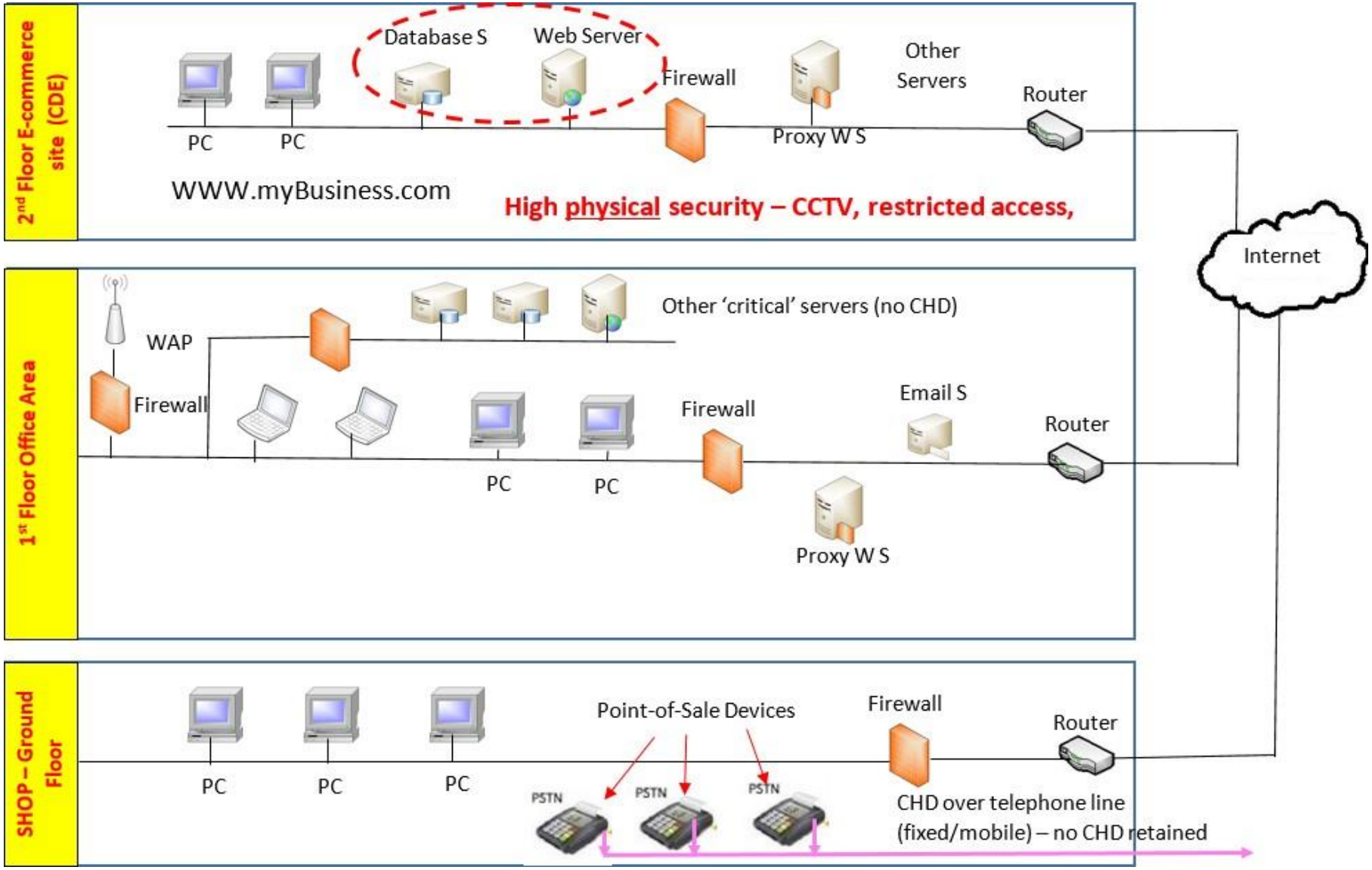
Let's conceptualize this 'API' strategy

PCI DSS – (3) Merchant managed e-commerce implementation



1. Merchant creates payment page.
2. Customer's browser displays the payment form.
3. The customer enters cardholder data into the payment form and the data is sent to merchant web server.
4. The merchant web server transmits cardholder data to the PSP.
5. The PSP receives cardholder data and sends it to the payment system for authorization.

A final example – more than online payments – what is the SCOPE of the PCI DSS coverage?



The Cardholder Data Environment

Any part of an organisation or merchant where its people, processes, and technologies store, process, or transmit payment card data, will be in scope for PCI DSS. This data will be classed as part of their Cardholder Data Environment (CDE).

As most data breaches involve a compromise of the CDE, PCI DSS requirements require a wide variety of security controls to be maintained to help protect this data.

In summary, the CDE consists of:

- All system components that store, process, or transmit Cardholder Data (CHD) or Sensitive Authentication Data (SAD).
- Any component that directly connects to CHD systems.
- Any component that supports CHD systems (such as anti-virus, authentication servers).

Clearly, PCI DSS auditing costs and data breach risk are both lowered by reducing the CDE to its bare minimum

PCI DSS Requirement 1.1.2 and 1.1.3: Network Documentation Best Practices

https://www.youtube.com/watch?v=4tW4p2mEKrw

Entertaining live phishing attacks

https://www.youtube.com/watch?v=sby_ZOat2GQ
https://www.youtube.com/watch?v=yhE372sqURU

Audio story: A Modern Cyber Attack

Listen as a fictional organization suffers and recovers from a GenAI enhanced phishing attack.

https://www.delltechnologies.com/asset/en-au/solutions/business-solutions/briefs-summaries/recover-from-a-cyber-attack-audiostory.mp3


```
        end;

    write(Endtext);
end.
CREATE TABLE product(
    class MultinomialNB(object):
    def __init__(self):
2})
        self.X = None
        self.y = None
    def __loading(self):
        self.list_labels = cl.Counter(
int acc(std::function<int(int, int)>
    auto it = operands.begin();
    int result = func(*it, *(++it));
    if (operands.size() > 2) {
        for (++it; it!=operands.end();
            result = func(result, *it);
        }
    }
    return result;
```

Thank you