MRC CERTIFIED PAYMENTS AND FRAUD PREVENTION PROFESSIONAL (CPFPP)

Study Guide

CPFPP | merchantriskcouncil.org

TABLE OF CONTENTS

INTRODUCTION 4

WHAT IS THE CPFPP CERTIFICATION? 4
- Why Does the Industry Need Certified Professionals? 4
- How the CPFPP Certification Was Developed 5
- Who Is Eligible to Sit for the CPFPP Exam? 5
- How the CPFPP Certification Benefits You 5
- Using the Study Guide 6

GETTING READY FOR YOUR EXAM 6
- Exam Structure 6
- Proctored Exams—Setup and Technical Requirements 6

SMART TEST-TAKING STRATEGIES 7
- Anatomy of a Multiple-choice Question 9
- How to Dissect a Question and Find the Correct Answer 9

EXAM DAY 10
- Getting Ready on the Big Day 10

GETTING YOUR RESULTS 10

WHAT HAPPENS NEXT 10

EXAM FOCUS AREAS 11
- Payments 11
- What Is Fraud? 12

DOMAINS OF PRACTICE 12

PERFORMANCE MANAGEMENT 12
- Fraud Investigation 13
- Payment Protocols for Secure Payments and Fraud Prevention 13
- Common Information Security Threats 15
- Sample Exam Questions 15

OPERATIONAL MANAGEMENT 16
Payment Processing Regulations and Requirements 16
Operations Management for Fraud Detection and Prevention 17
Investigating Fraud Patterns 18
Fraud Detection Techniques 18
Chargebacks and Representment 19
Sample Exam Questions 21

PROVIDER MANAGEMENT 21
What Are Payment Service Providers? 21
Contract Management 21
Fees and Fines 22
Processing Fees 22
Fraud Threshold Monitoring Programs 23
The Global and Regional Payment Ecosystem 24
Sample Exam Questions 25

FEATURES AND ENHANCEMENTS 26
Architecture and Flows Between Internal Systems/Services 26
Global and Regional Payment Methods and Their Pros and Cons 26
Payment Security and Compliance 27
Fraud Tools and Technologies 28
Components of a Contract 29
Product Roadmaps 29
User Experience (UX) and Workflow Requirements 30
Sample Exam Questions 30

GLOSSARY 31

ADDITIONAL RESOURCES 34
Exam Content Outline 34
Books and Websites 36

INTRODUCTION

Every company relies on their customers to succeed. Good customer relationships are based on trust, and a company's reputation is crucial to maintaining that trust. Fraud and payment misconduct can easily and quickly undermine a company's reputation, resulting in lost customers and potential legal or regulatory damage.

The Merchant Risk Council (MRC) is proud to offer the first-ever industry standard Certified Payments and Fraud Prevention Professional (CPFPP) Certification. This certification provides verified proof of expertise for anyone hoping to advance their career in these quickly growing industries. This study guide provides information and resources to help you prepare for the CPFPP certification exam.

WHAT IS THE CPFPP CERTIFICATION?

Certification is a voluntary process by which a non-governmental agency formally recognizes specialized knowledge, skills, and experience in a designated area as demonstrated through a standardized, comprehensive examination.

The purpose of the MRC CPFPP Certification is to provide verified proof of an individual's experience and knowledge related to:

- ☑ Payment ecosystems and eCommerce fraud concepts
- ☑ Transaction lifecycles
- ☑ Performance management
- ☑ Operations management
- ☑ Features and enhancements
- ☑ Provider management
- ☑ Payment orchestration and fraud management solutions and the value they provide

Meeting established criteria and passing the MRC CPFPP Certification examination demonstrates mastery of specialized knowledge in the field.

Why Does the Industry Need Certified Professionals?

As the technology powering payments continues to evolve, so do the attack methods utilized by fraudsters. Companies are challenged to stay aware of the types of threats that exist and the methods for identifying, investigating, preventing, and combating them. As consumers live busier lives, the demand for digital transactions grows in every business from financial management to travel to grocery shopping.

The number of digital platforms and frequency of transactions makes merchants and customers more vulnerable by the second and increases the need for experts who understand regulations, can detect vulnerabilities, implement effective preventative measures, and utilize appropriate response measures.

As regulations become more stringent, stakeholders are paying closer attention to risk management and the importance of payments and fraud prevention. While the payments and fraud prevention fields are large, the standardization and certification of knowledge raises your expected level of expertise.

How the CPFPP Certification Was Developed

For several years, the eCommerce community has requested a certification that recognizes payments and fraud prevention professionals as distinct specialized functions. After their own exploration of the need for industry standardization, the MRC leveraged its extensive institutional knowledge and relationships across the payments and fraud prevention industries to develop this unprecedented certification program.

The MRC engaged a team of subject matter experts to identify areas of competency for testing, develop appropriate test questions, and assist with the validation of the exams. The MRC Payments and Fraud Prevention Certification Program is dedicated to the validation of experience and a specialized body of knowledge for all professionals working as payments and fraud prevention professionals.

Who Is Eligible to Sit for the CPFPP Exam?

There are several ways to qualify to sit for the certification exam. The CPFPP exam eligibility pathways are combinations of payments and fraud management experience, undergraduate or graduate education, and professional training.

The eligibility pathways and additional training resources are provided in the downloadable CPFPP Candidate Handbook located on the Merchant Risk Council website. The handbook includes the application process, eligibility requirements, exam procedure, recertification requirements, and additional policies and guidelines.

How the CPFPP Certification Benefits You

The job and business markets have become a competitive global environment. Aside from conventional education, a professional certification gives you the advantage of validation from a third party. Professional certification:

- ☑ Increases your marketability as a job candidate or entrepreneur
- ☑ Increases your industry earning power
- ☑ Establishes or strengthens your reputation
- ☑ Gives you credibility as a subject matter expert
- ☑ Earns respect from professional peers

In the case of the MRC CPFPP certification, passing this rigorous exam that covers the most critical topics in payments and fraud prevention will help you stand out among your industry peers as having your knowledge tested and certified by well-known industry organizations. Read more about the significance of this certification and use of the certification mark in the CPFPP Candidate Handbook.

Using the Study Guide

This study guide has been developed to help you prepare for the CPFPP exam. It includes an overview of the exam structure, study strategies and test-taking tips, and an introduction to and review of the topics covered by the exam. The guide also includes a glossary of important payment and fraud industry terms, and additional resources. Please note that this guide is not an all-encompassing study resource. It is intended as a starting point from which you can determine the exam content area(s) you would like to focus your studies on. This guide does not include detailed information on testing procedures or MRC guidelines, which can be found in the CPFPP Candidate Handbook.

GETTING READY FOR YOUR EXAM

Exam Structure

The CPFPP certification exam consists of 115 multiple choice questions. Fifteen of these questions, dispersed throughout the exam, serve as pilot test questions, and do not affect the final score. The remaining 100 questions will be used to calculate the exam score. The percentage of scored questions are divided across four domains, shown below. A detailed exam outline and reference list is provided in the Additional Resources section of this study guide.

Domains of Practice	Percentage of Items
Performance management	**35%**
Operational Mamagement	**30%**
Provider Management	**20%**
Features and Enhancements	**15%**

Proctored Exam—Setup and Technical Requirements

A live proctored exam is a timed test monitored by a live person who guides test-takers through exam launch, verifies identity, and conducts a security scan of the testing environment so unpermitted materials can be removed before the exam.

The CPFPP exam is administered by the ProctorU live online proctoring service. To use ProctorU, you will need a high-speed internet connection, a webcam (internal or external), and a Windows or Apple operating system.

Before the exam, be sure the computer you plan to use allows you to download and install third-party software. Testing on a corporate computer is not recommended, as most corporate systems have internal firewall, permissions and security settings that might not be compatible with ProctorU's application.

The CPFPP Candidate Handbook provides instructions for registering with ProctorU, ensuring your computer will allow you to download the necessary software and test securely.

SMART TEST-TAKING STRATEGIES

Study time! The first step as you prepare to study is to consider how you budget your time and focus.

Once you have determined when you should study, use these techniques to help you review and retain the material:

- **Study in intervals**
  Avoid cramming in the days or hours before the exam, as cramming lowers your ability to retain information and causes anxiety. Studying in 20–50-minute increments with 5–10-minute breaks benefits long-term retention because it allows you time to process what you have read.

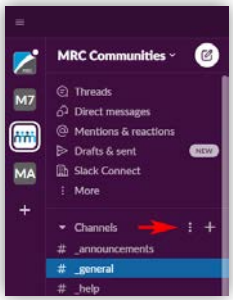
- **Remember that reading is NOT studying**
  Interact with the materials and think of the information as what you are learning and not just what you need to remember. Write your own thoughts about what you read to expand your perspective on the topic.

- **Test your expertise by explaining topics to another person**
  One of the best ways to review what you have learned is to put it into action by sharing it with others. By teaching what you study, you reinforce what you know and evaluate your understanding of the material.

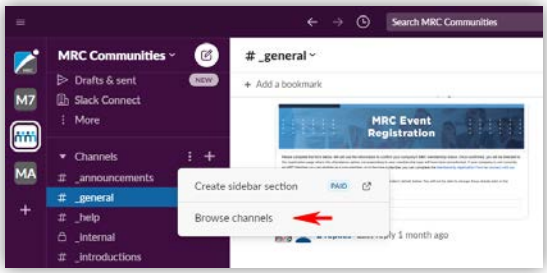
  The MRC offers a study group on Slack for people preparing to sit for the CPFPP exam. This is a great opportunity to share information, ask questions, and test your knowledge. Follow these steps to join the study group:

  1. If you do not have a Slack account, you will need to create one before joining.
  2. If you are not a MRC member, contact programs@merchantriskcouncil.org.
  3. If you are a MRC member, join the MRC Communities Slack workspace at: https://merchantriskcouncil.org/committees-and-communities/slack

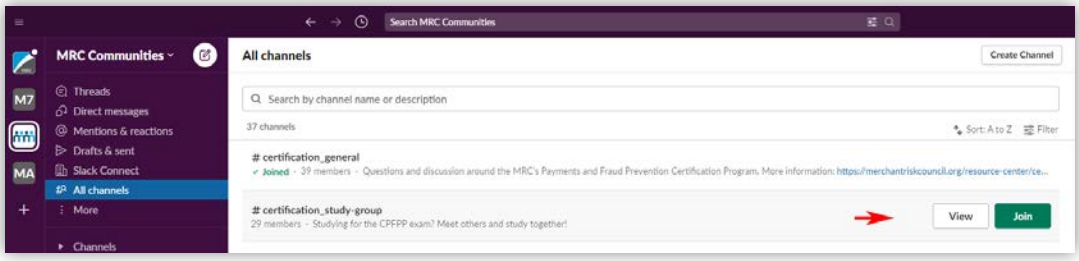
4. Once you have accessed the Slack workspace, hover your cursor over Channels on the left menu. When hovering, three vertical dots will appear.



5. Click on the dots and select “Browse channels”. A list of channels will appear.



6. Select the “#certification_study-group” from the channel list, and select “Join”.



Anatomy of a Multiple-choice Question

A multiple-choice question uses several parts. Within the body of the question are hints to what the correct answer should be. The parts of a question include:

- **Stem:** The problem posed by a test question presented in the form of a question or partial sentence. There should be a key indicator that will serve as a hint of what you should look for.
- **Answer:** The right answer choice.
- **Distractor or Foil:** Every choice other than the key answer. These incorrect or inferior alternatives should all be plausible to some degree but not so close to the right response that a reasonable case can be made for them.

How to Dissect a Question and Find the Correct Answer

Stem	What is chiefly responsible for the increase in the average length of life in the USA during the last fifty years?
Distractor	a. Compulsory health and physical education courses in schools
Answer	b. The reduced death rate among infants and young children
Distractor	c. The substitution of machines for human labor

In this example, the question asks for the circumstance that was CHIEFLY responsible for the increased length of life.

The distractors suggested reasons that could be attributed, but only one of the options (b), provided an option that could be directly related to the stem.

Read the stem: First, read the stem and make sure you understand the context.

Try to come up with the correct answer: Before you look at the answer choices, try to come up with the correct answer. This will help you to rule out choices that are like the correct answer. Now read and consider each option carefully.

Look for clues in the stem: Look for clues in the stem that suggest the correct answer or rule out any choices. For example, if the stem indicates that the answer is plural you can rule out any answers that are singular.

Eliminate any options you know are incorrect: Scan all the answer options first and eliminate those that clearly could not be an option. Eliminating options that you know are incorrect will help you focus on the remaining choices.

Come back to items you were unsure of: Skip questions you can't immediately answer with a reasonable degree of certainty. If you complete the entire exam with time to spare, go back to the skipped questions and review them again – you will often get clues (or even answers) from other questions.

EXAM DAY

Getting Ready on the Big Day

There are a few things you should do to prepare your mind, body, and environment to take your certification exam. While some of these may sound like normal daily activities, they go a long way in making sure you're ready.

- Get a good night's rest.
- Eat a well-balanced meal and avoid excessive stimulants such as caffeine.
- Take a walk or do a moderate workout the morning of the exam.
- Run a system check to make sure your computer is ready.
- Have a government-issued I.D. ready and be located in a private, well-lit room with no one else around you.
- Clear your workspace from all materials.

"What to Expect on Exam Day" in the CPFPP Candidate Handbook will tell you what to expect when you begin interacting with your exam proctor, what is permitted and prohibited during the exam, and what to do when your exam is complete.

GETTING YOUR RESULTS

Exam results will be provided via email. For reasons of privacy and confidentiality, examination results are released to the candidate only.

Individual score reports will contain an indication of "pass" or "fail" for the overall exam. If you did not pass, your score report will include information about your performance in each domain of the exam. If you do not pass, it is possible to retake the exam. More information on scoring, appeals, and re-testing is available in the CPFPP Candidate Handbook.

WHAT HAPPENS NEXT

Your certification will be valid for three years after the certification issue date.

Recertifying requires either re-taking the CPFPP exam or earning 60 CPE credits within the three-year period since the last certification was earned. At least 15 CPE credits required for recertification must be earned through the MRC (taking in-person workshops or MRC RAPID Edu online courses, speaking or presenting at MRC events).

EXAM FOCUS AREAS

This section provides an overview of payment methods used by merchants globally, and an introduction to fraud – both how it is defined and the way it is classified in the industry. Use this information as a primer for the remainder of the study guide, and as your foundational knowledge as a payments and fraud protection professional.

Payments

Merchants accept a variety of payment types, making in person and online transactions convenient for shoppers. The more frequently used payment methods include:

Wire Transfers are an interbank payment method. They involve sending money directly from one bank account to another. A wire is the simplest global payment method because it requires no middleman to handle the transfer, and the fastest method, as funds are received by the payee on the same day, or within 1-2 business days.

ACH, or Automated Clearing House, is a network that handles large batches of debit and credit transactions electronically. Domestic ACH transfers are a convenient, reliable, and inexpensive local payment method. ACH transfers are a cheap way to transfer funds between US bank accounts. It's often completely free to send and receive an ACH, and they're safer than wire transfers.

Global ACH, or International ACH, provides electronic funds transfer capabilities to dozens of countries, while payments are made in the local currency of the payee. Global ACH payments are sometimes called local bank transfers or direct to local bank transfers. These transfers are managed by the National Automated Clearing House Network (NACHA) and are required to follow all NACHA rules and standards.

Paper Checks instruct a bank to transfer a specific amount from the bank account of one party (the payer) to another party (the payee). The payee can then cash the check or deposit it directly into their own bank account. Funds are not withdrawn until the payer's bank receives the check, determines the drawer has money in their account, and releases the amount to the payee.

Mobile Wallets or eWallets are used for ePayments both domestically and internationally. Mobile wallets facilitate ecommerce, promote online shopping, and streamline online purchases. Some wallets facilitate funds being withdrawn from the payer's account (usually via ACH) and loaded into their account, while others offer the ability to store your credit cards on your phone to make purchasing on a mobile website or app easier and more secure.

Credit/Debit/Prepaid Cards use a debit card provider network. Funds are drawn from the payer's managed account and transmitted to the payee's debit card account. The payee can then use those funds to pay for goods and services that accept card payments at checkout or a POS (usually in partnership with Visa or Mastercard). Funds are received immediately but may be held by the debit card provider if there are issues.

What Is Fraud?

"Fraud" is any activity that relies on deception to achieve a gain. As defined by Black's Law Dictionary, fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment". It is often assumed that fraud is always intentional and always looks the same, but fraud presents differently depending on the circumstances.

Transactions flagged as fraudulent can be classified as true fraud or first-party misuse.

True fraud is a specific case of a customer's identity, login credentials, or card being stolen and used to acquire funds or goods and/or services without their knowledge.

In a **first-party misuse** or "friendly fraud" scenario, the genuine customer is disputing a transaction due to confusion (e.g., they don't recognize a purchase or billing descriptor on their credit card statement), or are simply attempting to take advantage of a merchant. A common example of first-party misuse is without the cardholder's knowledge, a child uses their card to make a purchase and the customer reports the purchase as unauthorized).

While these are two widely different scenarios, both types of fraud can result in a chargeback to the merchant. It is important to investigate the circumstances surrounding the transaction to make sure merchants know how and when to defend a chargeback.

DOMAINS OF PRACTICE

PERFORMANCE MANAGEMENT

Performance management is key to successful payments and fraud prevention. There are a set of key metrics that define how a well-run payments and risk organization is structured:

Payment Authorization Rate – How many people are being approved when they attempt to purchase your product, and how many are being rejected. This metric is directly linked to revenue coming into a merchant's business.

Risk Rejects – How many times is a merchant's risk service rejecting a customer because they suspect they are a fraudster. It is important to know if rejections are people committing fraud or if they are false positives (good customers being blocked), and how to measure and balance between the two.

Cost of Payments – How much it costs a merchant to process transactions inclusive of those who must be paid (banks, processors, card brands, gateways, acquirers, employees, etc).

Fraud Rate – Normally measured by chargebacks, gross fraud rate is measured by chargebacks received/settled transactions, while net fraud rate removes the chargebacks that are successfully disputed (after fees and operating expenses).

Cost of Fraud – Measurement of cost of fraud to a merchant (lost chargebacks, fees, false positives) and fraud prevention measures (staff, tools, data).

Examining these key performance indicators help to set up criteria, workflows, and protocols for effectively identifying, minimizing, and addressing fraud activity.

Fraud Investigation

Investigating fraud starts with linking data attributes around a transaction. Whether the data being used is internal to the organization or provided by external sources, the context around a transaction (IP address, device used, age of account, previous use of payment method, etc.) can be used to identify good customer patterns vs. bad actors.

A fraud investigator can use contextual data and look elsewhere (previous purchases, use of products, links to other accounts) to identify behaviors and repeat patterns that can reveal fraud activity. They can also engage external sources (fraud services, external data repositories or chargeback service providers) who may be able to advise on data attributes that are not common inside the organization.

Payment Protocols for Secure Payments and Fraud Prevention

ISO 8583

The ISO 8583 message is an international standard for financial transaction, card-originated interchange messaging. It is the International Organization for Standardization standard for systems that exchange electronic transactions made by cardholders with credit or debit cards. In short, this is the data shared by merchants and banks to communicate a credit card transaction.

ISO 8583 defines a message format and a communication flow that allows systems to exchange transaction requests and responses. Most transactions made when a customer uses a card to make a payment in a store or at ATMs use ISO 8583 at some point in the communication chain. The Mastercard and/Visa networks base their authorization communications on the ISO 8583 standard, as do many other institutions and networks.

It is important to understand the original intention of ISO 8583. ISO 8583 was built in the 1980s to facilitate in-store credit card transactions. This is a standard that was developed before the advances of eCommerce technology, so common eCommerce data elements such as IP address and email address are not inherently present.

3D-Secure

With the increased popularity of eCommerce platforms, many transactions that would have previously occurred in person are now made online. While this makes shopping and business more convenient for consumers and allows merchants to grow revenue faster, it brings with it an increased risk of payment card fraud.

3D-Secure (3DS) is a security protocol used to authenticate users and provide additional information to banks for card-based transactions in card-not-present (CNP) scenarios.

The process was designed to authenticate a cardholder's identity to prevent payment fraud, hinder unauthorized transactions, and reduce chargebacks. In a 3DS transaction, the cardholder may be asked to provide proof of identity by entering a unique password, SMS code, temporary pin, or to log in to their bank's mobile app.

It is important to note that 3DS transactions shift the fraud liability of the purchase event to the issuing bank. While this may sound like a win for merchants, it also typically results in a much lower payment approval rate and higher customer abandonment rate, which is why 3DS is seldom used in countries where it is not mandated by government regulation. As of 2022, Europe is the only major market where the government mandates all merchants use 3DS for eCommerce transactions. It is also important to note that merchants can lose the liability shift benefit if they are allowing excessive fraud as determined by the card brands.

Transaction Optimization

Transaction optimization is a complex process that is highly valuable to merchants. When an eCommerce merchant sends a transaction to a bank, transaction optimization can address and correct the information that might cause a card to be declined.

Many large organizations have access to an optimization tactic called Real Time Account Updater. Originally created to manage subscriptions (e.g. Netflix or Amazon Prime), this tool can retry card information by contacting a card issuer to retrieve the correct information – such as an incorrect expiration date – and update the information so that a transaction can be approved, all without involving a customer.

Common examples of transaction optimization tactics are:

- ☑ Dynamic retry (retry a declined transaction over another acquirer to try for an approval)
- ☑ Tokenization (swap the card number for a network-issued token to ensure all card details are automatically updated when the card is changed)
- ☑ Account updater (proactively receive new card numbers and expiration dates from banks when a card has been updated)
- ☑ MID/MCC switching (send specific transactions through a different Merchant ID or Merchant Category Code to fetch a higher approval rate)
- ☑ Alternate routing (label a dual-purpose card transaction as debit or credit to try and fetch the highest possible approval rate for that card)
- ☑ Removing optional data from the authorization message (remove data such as billing address, expiration date or CVV to fetch a higher approval rate)

While many of these optimization tactics can result in higher payment approval rates, they can also result in higher levels of fraud. It is important for payment and fraud prevention professionals to pay close attention to performance metrics as they test and learn the right optimization strategy for their specific business.

Payment Performance Benchmarking

Merchants should strive to have relationships with their acquirers, the major card networks, and major card issuers to benchmark their approval rates and fraud rates to determine how

they are performing compared to their industry or vertical. Providers can provide benchmark analysis that helps merchants build a roadmap to greater approval rates.

Common Information Security Threats

Technology has created opportunities for fraudsters to attack consumers and merchants using a variety of techniques. Some of the most common threats that users need to be educated on and constantly aware of include:

Phishing - The practice of sending emails purporting to be reputable companies, aimed at inducing individuals to reveal personal information, such as passwords and credit card numbers.

Social Engineering - Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks, or physical locations or for financial gain. While fraud prevention and risk professionals understand social engineering tactics, it behooves them to educate other teams on recognizing and addressing social engineering methods. This is particularly important for customer service teams who are a strong target for social engineering, as customer relationships are critical to their success.

Dark Web - The dark web refers to encrypted online information that is not accessible via conventional search engines. The dark web can only be accessed using specific browsers. While it is intended to keep internet activity anonymous and private, it can be used for both legal and illegal applications.

Ransomware - Malware used by cyber attackers to encrypt information and deny a user access to files on their own device until a ransom is paid for a decryption key to regain access to their files.

These fraudulent behaviors illustrate why it is so important for merchants to establish fraud metrics, and build and maintain strong fraud prevention policies and protocols.

Sample Exam Questions

1. What type of fraud scheme is facilitated through social engineering?
   - **a.** Counterfeiting credit cards
   - **b.** Engaging in romance scams
   - **c.** Manipulating point of sale devices

2. For what reason can a payment response code for insufficient funds appear?
   - **a.** When there is not enough to cover and complete the current payment
   - **b.** When the wrong CVV is entered
   - **c.** When there was an outage on the network, and the control was taken by the “stand-in” system

Answers: 1-b, 2-a

OPERATIONAL MANAGEMENT

Operational management consumes transactional data and uses that data to benchmark activity against KPIs to identify anomalies in transactions. These anomalies are used to either fix an issue or to determine if another solution is needed. Operations teams can work heavily with payments and fraud professionals to facilitate the data that card processors provide to their organization.

Examining data means looking at current vs. historical data to find anomalies such as higher or lower acceptance rates and finding out the cause of those differences. This is how fraud is found.

Payment Processing Regulations and Requirements

As most consumers pay for their purchases using debit and credit cards, and with the number of eCommerce transactions that take place daily, the government and credit card industries maintain a strict set of regulations and requirements designed to protect the interests of both merchants and consumers.

Payment mandates are designed to protect the integrity of payments by improving customer experience and making fraudulent transactions more difficult. Credit card brands typically generate revenue from payment mandates, so not being aware or in compliance can be costly.

Card network rules are the rules and standards that apply to debit card or credit card network participants and specify the requirements and limitations for participants of a debit card or credit card network system. They include the American Express Business and Operational Policies, Visa Core Rules and Visa Product and Service Rules, and Mastercard Rules and Mastercard Transaction Processing Rules.

While the major credit card issuers maintain their own evolving sets of requirements, there are regulations that merchants must comply with if they accept debit or credit cards. They include:

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a global data security standard required of all businesses, regardless of size, that accept credit cards. PCI DSS and the Payment Application Data Security Standard (PA-DSS) are rules designed to reduce the incidence of credit card fraud. PCI compliance requires merchants meet the following requirements:

- ☑ Install and maintain a firewall configuration to protect cardholder data.
- ☑ Do not use vendor-supplied defaults for system passwords.
- ☑ Protect stored data.
- ☑ Encrypt the transmission of cardholder data across public networks.
- ☑ Use and regularly update top antivirus software or programs.
- ☑ Develop and maintain secure systems and applications.
- ☑ Restrict access to cardholder data on a business need-to-know basis.

- ☑ Assign a unique ID to each person with computer access.
- ☑ Restrict physical access to cardholder data.
- ☑ Track and monitor all access to network resources and cardholder data.
- ☑ Regularly test security systems and processes.
- ☑ Maintain a policy that addresses information security for all personnel.
- ☑ Both the PCI DSS and PA-DSS are enforced by the PCI Security Standards Council, an independent body created by the four major credit card brands.

PA-DSS
PA-DSS mandates that all point-of-sale (POS) equipment and terminals comply with PCI DSS standards. PCI compliance is normally included with POS hardware.

Durbin Amendment
The Durbin Amendment is part of the Dodd-Frank law passed by Congress in 2010. Its purpose is to protect consumers by lowering the interchange fees on debit card transactions, which have the lowest risk of fraud and therefore, lawmakers argued, should be much less expensive than riskier transactions.

Merchants should pay attention to regulatory changes each year, and along with their own internal payments and fraud management policies and practices, use them to protect the interests of themselves and their customers. Merchants should also be asking their acquirers to provide them with quarterly (at minimum) summaries of all new applicable regulatory and card mandate changes.

Operations Management for Fraud Detection and Prevention

It is important for operational management teams to have direct relationships with an organization's partners, and that they establish monitoring and alerting systems to convey issues related to data that the rest of the business should be aware of.

Finding fraudulent activity requires watching trends daily. Operations teams can see trends and behavior that necessitate a deeper investigation to determine if the fraud is malicious or first party misuse. Determining fraud is not based on a finite set of circumstances. Operations teams take a critical view of data to find patterns that might not be as easily picked up in standard daily reports.

Operations is also primarily responsible for ensuring the correct data is being provided by the processors. The type of data provided by processors depends on the agreement between the processors and the organization, but operations can specify the type of data processors should provide. New data points can also be requested.

For example, if the processor is not providing the merchant with AVS or CVV result fields, the merchant would want to address this to make sure they do.

Investigating Fraud Patterns

Payment and fraud professionals utilize a variety of methods to identify fraud patterns and determine the level of risk for their organization.

Trends and Patterns – Internal measurement of a company's current performance trends and benchmarking data to compare to patterns over time.

Business and Industry – Engaging a third-party provider who can provide higher level anonymized data to give a snapshot of performance in a business category. This allows operations to see how their organization is trending against their industry.

Customer Experience Against Rising Fraud Threats – In many organizations, fraud investigation teams are plugged into customer experience teams, to get a gauge of fraud through customer behavior and complaints. Trends in unusual issues should trigger an investigation – this is where many fraud threats are identified. For example, multiple people reporting that they don't have an account with an organization is an indicator of a potential larger fraud ring.

When larger fraud activity is found through an investigation, the organization's internal or third-party risk engine can be fine-tuned to flag certain behaviors and patterns to limit that rising fraud threat.

Fraud Detection Techniques

Data Analysis

There are several common types of analysis done by a fraud ops team, such as:

- **Statistical Parameter Calculation**
  The calculation of statistical parameters such as averages, performance metrics, and probability distributions for fraud-related data collected during the data capturing process.

- **Regression Analysis**
  Regression analysis allows fraud investigators to examine the relationship between two or more variables of interest, to understand and identify relationships between several fraud variables. This further helps predict future fraudulent activities.

- **Probability Distributions and Models**
  Models and probability distributions of various businesses fraudulent activities are mapped, either in terms of different parameters or probability distributions.

- **Data Matching**
  Data matching is used to compare two sets of collected data. The process can be carried out either based on algorithms or programmed loops. Data matching also removes duplicate records and identifies links between two data sets for marketing, security, or other purposes.

AI-based Techniques

Artificial Intelligence (AI) for fraud prevention has played a key role in helping companies enhance security and streamline business processes. Through improved efficiency, AI has emerged as an essential technology for preventing fraud at financial institutions. AI fraud detection techniques include:

- **Data Mining**
  Data mining classifies and segments data and finds associations and rules in the data that may expose potentially fraudulent patterns.

- **Neural Networks**
  Neural networks perform classification, clustering, and forecasting of fraud-related data that can be compared against information found through internal audits or within financial documents.

- **Machine Learning (ML)**
  Machine learning (ML) for fraud detection uses algorithms and models to learn from historical fraud patterns to assist with recognizing behaviors in future transactions. ML is applied using supervised or unsupervised learning methods and is usually supervised by data scientists.

  Supervised learning takes a random subsample of all records manually classified as either 'fraudulent' or 'non-fraudulent'. Unsupervised learning seeks common patterns (i.e., fraudulent) and correlations in raw data, and predictions are built without additional labeling.

- **Pattern Recognition**
  Pattern recognition algorithms detect approximate classes, clusters, or patterns of suspicious behavior, either automatically (unsupervised) or manually (supervised).

Chargebacks and Representment

A **chargeback** is a credit or debit card transaction that the customer disputes with their issuing bank. Chargebacks usually result in a fee assessed to the merchant. Chargebacks can have a variety of reason codes associated to them by the issuing bank, but at a high level are either "fraud" chargebacks (the customer claims they did not make the purchase) or "non-fraud" chargebacks (the customer does not believe the merchant delivered the goods or services in the manner that was disclosed to them).

In the U.S. debit card chargebacks are governed by Regulation E of the Electronic Fund Transfer Act, and credit card chargebacks are governed by Regulation Z of the Truth in Lending Act. Because of these regulations merchants and banks are required to respond to customer chargebacks in a timely manner.

Chargeback representment is the process in which a merchant submits evidence to the issuing bank to prove that a chargeback is illegitimate. The bank will evaluate the information or evidence presented by the merchant and determine if the chargeback should be reversed.

Representment is the most important phase of the chargeback process for merchants. The parties involved in the process are the customer who raises the complaint with the issuing bank; the issuing bank which alerts the acquiring bank; and the acquiring bank which notifies the merchant. The methods for analyzing and disputing chargebacks include success metrics, reason codes, and compelling evidence rules.

- **Success metrics**
  A merchant's success metric is their representment win rate, which is a key metric. Merchants use success metrics to help identify the types of cases that are worthwhile to dispute, as there is a cost for representing a chargeback.

  How many cases are being won? How many cases are being lost? Among those being lost, what factors do they have in common? Is there a common piece of compelling evidence that should be included, or should these cases not be represented?

- **What are reason codes?**
  A chargeback reason code is a two-to-four-digit alphanumeric code that identifies the reason for the dispute. Each of the major credit card issuers (Visa, Mastercard and others) use their own system of reason codes. The codes help merchants determine their strategy for addressing recurring chargebacks, decide if a chargeback should be represented, and identify frivolous chargebacks that they will want to dispute.

  Reason codes can range from very broad to very specific reasons, including lost and stolen cards, goods not as described, not received, etc. There are cases when a chargeback is given a general reason code, such as "customer does not know." In instances when this kind of code is frequently used, the merchant is left unable to thoroughly investigate an issue or gather compelling enough evidence to support a potential chargeback dispute.

  The goal of the reason code system is to eliminate guesswork and opinion-based decisions. Established chargeback reason codes do a good job of addressing processing errors, merchant fraud, and other "legitimate" reasons for filing a dispute. But chargebacks are increasingly being filed for reasons that have little to do with the assigned chargeback code.

- **Compelling evidence rules**
  Compelling evidence is a represented chargeback that includes more than just transactional data to support the dispute. Merchants can compile a compelling evidence package with detailed information supporting the argument that the fraud liability should lie with the issuing bank or end customer.

  Types of compelling evidence can include results of fraud prevention checks, customer authentication methods, previous purchase records, or case-by-case evidence like confirmation of delivery. Banks are looking for the strongest pieces of evidence.

When a customer initiates a chargeback, the merchant must respond within a set period. The period varies by the card brand but is typically 30 days. When responding, the merchant can provide any evidence that the transaction is legitimate, including signed receipts, contracts, and any other documentation that shows that the chargeback is in error.

Representment can be considered a fraud prevention policy because when well executed, it can prevent repeat cases of malicious fraud. The effort and cost associated with fraud investigation and chargeback representment illustrate the importance of building and maintaining a strong risk management policy.

Sample Exam Questions

1. Which stakeholder makes the final determination whether a chargeback is a fraud chargeback or a service chargeback?
   a. Customer
   b. Card network
   c. Issuing bank

2. What stakeholder initiates a 10.5 Visa chargeback?
   a. Card network
   b. Cardholder
   c. PSP

Answers: 1-c, 2-a

PROVIDER MANAGEMENT

What are Payment Service Providers?

Payment Service Providers (PSPs) make it possible for businesses to accept a variety of online payments, including credit, debit, cash cards and eWallets.

PSPs provide services that enable essential business tasks, but rarely interact with clients. Provider management involves a team of experts, software, and tools for managing payments, identifying, minimizing, and managing fraud. This can lead to better accuracy and reduced risk and liabilities.

Contract Management

Credit and debit card processing is a critical revenue driver for merchants and required for eCommerce businesses. A well-negotiated credit card processing contract can be cost-effective and enable merchants to accept credit card payments for their products or services at a fixed, predetermined fee schedule. Some merchants have direct contracts with the payment networks outside of their PSPs and acquirers.

Conversely, a contract can also contain fine print that if not understood can cost merchants hidden fees and percentages. Here are some important considerations for merchants when negotiating a new PSP relationship:

- ☑ Obtain a fair pricing structure.
- ☑ Review your terms and conditions.
- ☑ Work with a dedicated account manager.
- ☑ Seek a variety of payment solutions.
- ☑ Demand flexibility and adaptability.

Fees and Fines

There can be many costs associated with credit and debit card processing. Many of these are part of contract negotiations between merchants and card processors, while others are assessed and regulated by credit card issuers or governments. They include:

Processing Fees

Merchant's pay **credit card processing fees** for each card transaction. These fees are split among the financial institutions that enable credit card payments. Processing fees include interchange, assessment, and payment processing.

Interchange fees are transaction fees that a merchant's bank account must pay when a customer makes a purchase with a credit or debit card. Interchange fees are paid to card-issuing banks to cover handling, fraud. bad debt and risk management costs.

Card-issuing banks, payment processors (which may or may not be the issuing bank), credit card payment networks like Mastercard and Visa, payment gateways, and the merchant's own bank will all charge a percentage-based fee on every transaction. These charges often appear as a single, bundled amount on the merchant's bill. Given the wide range of transaction types, there are approximately 300 individual interchange fees that comprise the single interchange fee billed to a merchant.

Based on the costs of moving money, the **time value of money** in terms of current interest rates, and the relative risk involved, credit card companies set and regularly adjust their interchange rates. There are several factors that can affect interchange rates:

- **Card type:** Debit cards with PINs have lower rates than credit cards due to lower risk, and each credit card company will charge a different rate.
- **Business size and industry:** Rates can vary by Merchant Category Code (MCC), which are codes that payment brands use to classify merchants and businesses by the type of goods or services provided (supermarkets, for example, pay more than do gas stations). Debit cards in general have lower rates compared to credit.
- **Transaction type:** POS (point-of-sale) transactions are less risky than CNP (card-not-present) since EMV chips can be scanned.

Merchants are charged **assessment fees** on the total of their monthly sales for each credit card brand. Sometimes referred to as a "swipe fee", the fee is paid entirely to credit card associations for accepting and processing their credit cards at a merchant's place of business. Interchange Fees and Assessments are the same for all merchants, regardless of the size of the merchant or the amount of credit card volume processed.

A **foreign transaction fee (FTF)** is a surcharge credit card holders pay for cross-border transactions processed outside the United States. These can be purchases consumers make while traveling abroad or online from a merchant that is based overseas.

Foreign transaction fees are composed of two charges. One comes from the card issuer—for example, Chase, Bank of America, or Citi. The other is from the network: Visa, Mastercard, Discover or American Express. Every credit card will have varying terms that dictate how much a foreign transaction fee will cost the cardholder, so it's important to review your credit card's terms and conditions to know exactly how much you'll be paying.

Foreign transaction fees can be confused with the fee consumers pay for currency conversion. However, **the foreign transaction fee is a separate fee that is paid on top of currency conversion rate**.

Fraud Threshold Monitoring Programs

When merchants accept Visa cards, they are responsible for controlling and preventing fraud. When merchants generate excessive fraud or dispute activity, Visa places them in the Visa Dispute Monitoring Program (VDMP) or Visa Fraud Monitoring Program (VFMP). Failure to meet the requirements to exit the monitoring programs can result in fines/fees, loss of chargeback representment rights, loss of 3D Secure liability shift, remediation plan requirements, and ultimately if not remedied, loss of processing privileges.

VDMP levels are measured by:

- **Early warning:** dispute ratio of 0.65% and at least 75 total disputes
- **Standard:** dispute ratio of 0.9% and at least 100 total disputes
- **Excessive:** dispute ratio of 1.8% and at least 1,000 total disputes

Dispute ratio is calculated by dividing the number of disputes by the total number of transactions.

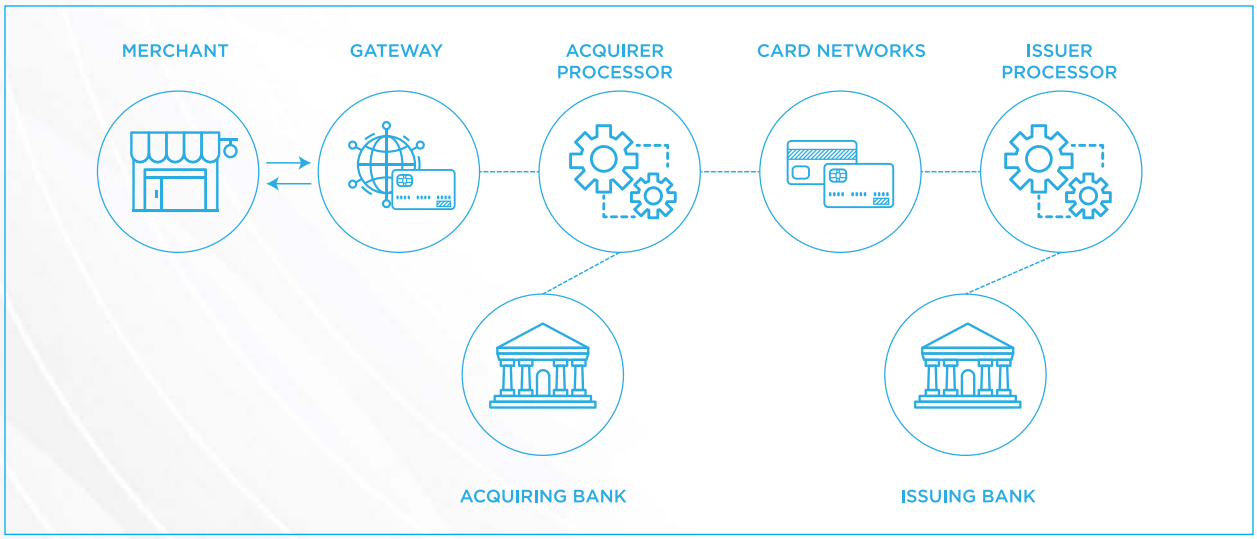
VFMP is measured by fraud coded chargebacks and TC40 data

- **Early warning:** fraud rate of 0.65% and at least US$50,000 in total fraud
- **Standard:** fraud rate of 0.9% and at least US$75,000 in total fraud
- **Excessive:** fraud rate of 1.8% and at least US$250,000 in total fraud

Fraud rate is calculated by the monetary value of fraud transactions divided by the monetary value of total transactions.

The Global and Regional Payment Ecosystem

Merchants accept many credit and debit card payments daily. While the process is fast and simple between the merchant and the customer, there are several interactions happening between multiple players behind the scenes. The payment ecosystem is the interconnection of networked electronic equipment, banks, and non-banking financial corporations to facilitate the transfer of funds between customers and merchants. The players in the payment ecosystem include:



Acquiring Bank: The acquiring bank is the financial institution that receives the funds customers have paid by retrieving money from the issuing bank. In short, the issuing bank is the customer's bank and the acquiring bank is the merchant's bank. The issuing bank is the financial institution that provides the customer with the credit or debit card they use to make payments. When a transaction is authorized, the issuer transfers the money to the acquirer, who brings it to the merchant.

Acquirer Processor: The acquirer processor authorizes transactions and receives transaction settlement information. Processors link the merchant, card scheme or APM and acquirer; evaluates whether transactions are valid and approved by the issuer; and works to minimize fraud and chargebacks.

Cardholders: The customer and holder of the card who pays a merchant for goods and services.

Card Issuer or Issuing Bank: A financial institution that provides a card to a cardholder and administers use of the card. The card issuer is also the merchant's banking partner.

Card Network (debit): A debit network is an electronic network that permits several types of financial transactions, including ATM cash withdrawals, debit card transactions, and online bill pay. Debit card transactions require electronic communication between banks for authentication and processing purposes. Because of the wide range of banks and banking systems, many different debit card networks have come into being over the years. Some of the most prominent networks are Star/Accel, NYCE, Pulse, and Interlink.

Card Network (credit): A payment network is an association of member banks that facilitates the payment transaction between the merchant, issuer, and source (issuing bank) of funds. While some credit card networks are also issuers, not all credit card networks issue credit. Visa and Mastercard are not card issuers, they are strictly payment networks; American Express and Discover are both issuers and payment networks.

eCommerce Marketplaces: An eCommerce marketplace is software that enables purchasing and selling over the internet. These platforms provide merchants with a central location for managing their virtual assets, digital sales, and marketing. There are multiple types of ecommerce platform solutions, and each type has unique benefits and advantages. The three main types of eCommerce platform are:

- Subscription-based
- Open-source eCommerce platforms
- Headless

Independent Sale Organization (ISO) or Payment Service Provider (PSP): Non-banking financial organizations that are affiliated with banks and card networks. These entities resell payment processing services to merchants; they also provide merchants with online payment gateways and POS devices.

Issuer Processor: An issuer processor connects with the card schemes and issuing banks to manage card issuance, authorize transactions, provide records, and communicate with all the different clearing and settlement parties.

Merchant: Seller of goods or services who accepts credit or debit cards for payment

Payment Gateway: A payment gateway is a virtual credit and debit card reader that transfers data between a terminal, website, or mobile device to the payment processor to continue the payment lifecycle.

Sample Exam Questions

1. What is the purpose of the Payment Services Directive 2 (PSD2)?
   a. Strong customer authentication
   b. Require 3DS
   c. Real-time payments

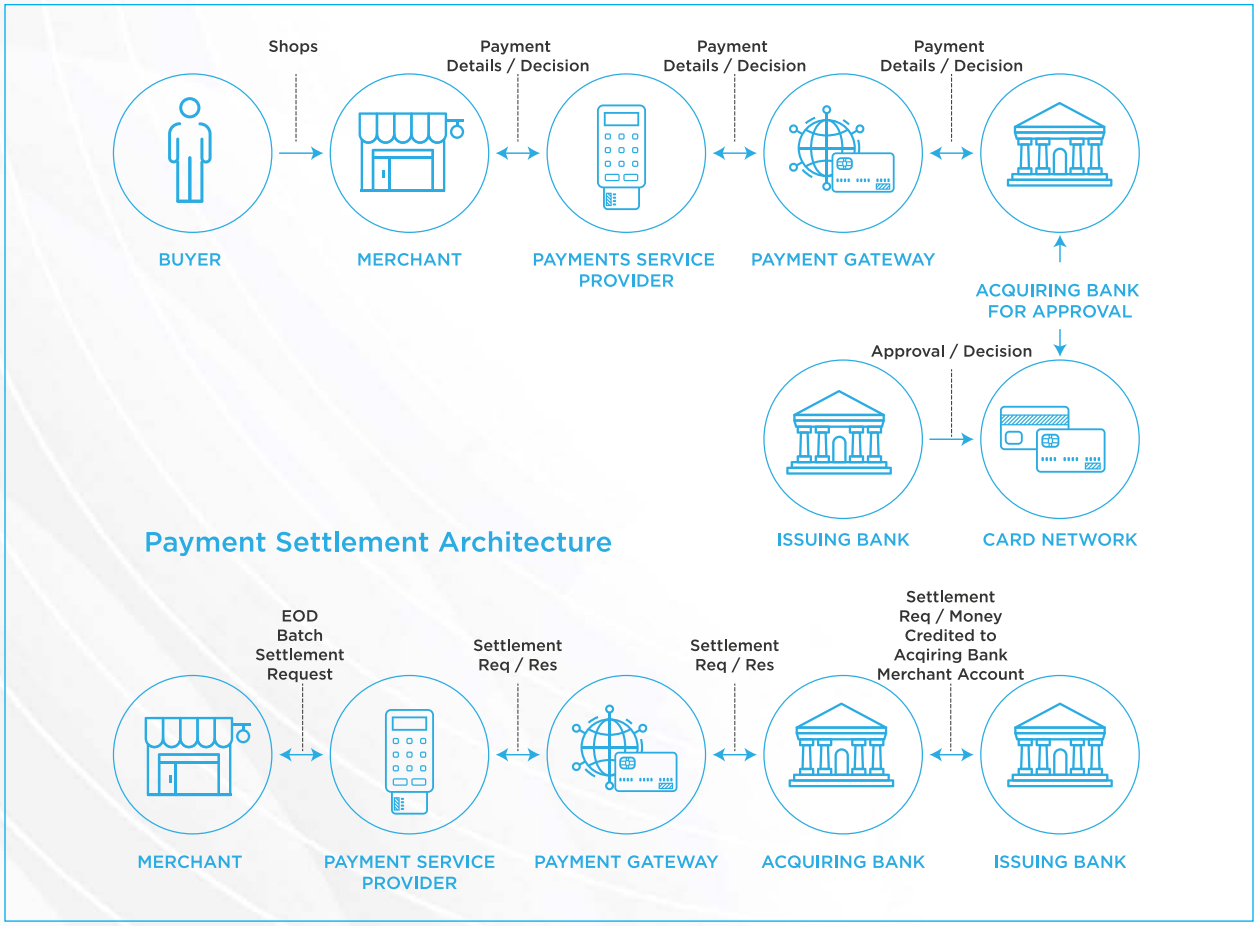
2. Which of the following describes the relationship between the exchange rate and the transaction costs?
   a. Transaction costs include exchange brokers' commissions and exclude "spreads" charges by brokers and foreign exchange dealers
   b. Transaction costs include exchange brokers' commissions and "spreads" charges by brokers and foreign exchange dealers
   c. Transaction costs include exchange brokers' commissions and "spreads" charges by brokers, foreign exchange dealers and insurance brokers

Answers: 1-a, 2-b

FEATURES AND ENHANCEMENTS

Architecture and Flows Between Internal Systems/Services

Payment processing is the flow that a transaction follows when a customer swipes their debit, credit card, or eWallet. Following is the flow of payment information between internal systems and services:



For more information on the steps or participants in the above flow, see the section on the Global and Regional Payment Ecosystems.

Global and Regional Payment Methods and their Pros and Cons

There are thousands of global payment rules for suppliers across the world. The best payment method typically depends on where the supplier is located and their expectations. A business needs multiple global payment methods because vendors are looking for a flexible payment experience to best suit their needs. Merchants are more frequently using payment "families" that offer customers multiple payment options. Payment method families include:

- Mobile Wallets
- Bank Debits
- Bank Credits
- Bank Redirects
- Bank Transfers

- Buy Now Pay Later (BNPL)
- Cash Based Vouchers

There can be several pros and cons with payment methods, depending on the type of business and the type of transaction. Those pros and cons include:

- Funding or settlement timing (immediate or 1-2 business days for decisioning)
- Some payment methods support disputes (aka chargebacks) and some don't
- Some payment methods naturally meet SCA (Strong Customer Authentication) requirements which require customers to prove identity prior to transaction approval
- A payment method may or may not support recurring payments
- A payment method may or may not support refunds
- A payment method may or may not support broad international acceptance or may have regional limitations

Payment Security and Compliance

Payment security compliance refers to the technical and operational standards that businesses must follow to secure and protect cardholder's credit card data when it is transmitted through card processing transactions. There are several processes and regulations that businesses follow, including:

Bank Card Issuing

Each cardholder has their own data set- account number, spending limits, plus 'profile' information, for example. A profile defines which cryptographic keys are to be used, settings for PINs, and risk parameters. The card issuer needs to be in control of all security aspects and cryptographic keys.

It is important to note that the three-digit CVC security code (located on the back of a physical card) cannot be stored by anyone in the approval process, including the Payment Service Provider who stores the personal account number (PAN) and expiration date.

The California Consumer Privacy Act of 2018 (CCPA)

The CCPA gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers.

General Data Protection Regulation (GDPR)

The GDPR is legislation that updated and unified data privacy laws across the European Union (EU). GDPR was approved by the European Parliament on April 14, 2016 and went into effect on May 25, 2018. This regulation requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.

Key Injection for Points of Interaction

PCI compliant attested devices are the starting point in the secure payment processing chain, initiating a non-repudiable and tamper-protected transaction. To make sure device identities cannot be hacked, the keys need to be generated by an HSM.

PCI Compliance for eCommerce
PCI compliance is the set of technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.

Secure Electronic Payment Services and Open Banking
Important new entrants in the transaction landscape are Payment Service Providers—third-party companies that provide services to manage payments. It is essential that payments are processed in a safe and reliable way.

Sarbanes-Oxley Act
The Sarbanes Oxley (SOX) Act of 2002 was passed by the United States Congress to provide security for consumers and the public against corporations acting maliciously or carelessly. The general requirements of SOX compliance are geared towards ensuring that companies are transparent when it comes to financial reporting and that there are more official rules in place to prevent fraud.

Strong Customer Authentication (SCA)
The SCA rule went into effect as of September 14, 2019, as part of PSD2 regulation in Europe. The rule requires changes to how European customers authenticate online payments. Transactions that don't follow the new authentication guidelines may be declined by a customers' bank.

Fraud Tools and Technologies

Merchants may utilize tools to identify fraud via contracts with external solution providers or may work with their development teams to build tools in-house.

Device Intelligence
Information about a device such as device type, operating system, software, hardware, settings, location, and history used to determine trusted customers and known or suspected bad actors.

Behavioral Biometrics
Analysis of a user's session behavior to identify anomalies between behavior typical of legitimate customers to that of potential bad actors or automated bot driven fraud attacks.

Rules Engines
Apply scores to transactions that determine an action such as automatic acceptance, automatic rejection, or queuing for review by an analyst. Rules can be configured by the merchant or managed by the service provider.

Data and Identity Validation
Tools that provide information or risk scores associated with specific data elements such as email address age, validity, reputation, or information on billing addresses, phone numbers, etc. Can be automated and incorporated into other fraud tools or queried by investigators and analysts.

Components of a Contract

Some of the important considerations in a contract between a merchant and a solution provider include:

- ☑ **Term** – The start and end date of the agreement.
- ☑ **Renewal** – The process for renewing the agreement (if the merchant wishes to renew). For example, whether the merchant elects automatic contract renewal automatic or if action will be required.
- ☑ **Termination** – The process and requirements for merchant to terminate an agreement Performance-related incentives or penalties tied to metrics such as accept/reject rates, fraud or chargeback rates, accuracy.
- ☑ **Guaranteed Minimums or Exclusivity**
- ☑ **SLAs (Service Level Agreements)** – Define service expectations and the metrics by which they are measured as well as remedies available for non-performance. Common SLAs in fraud management:
  - Network availability or 'up time'
  - Capacity - does the provider have the capacity to handle a merchant's traffic volume, particularly during spikes like high-demand sales, promotions, Black Friday, etc.
  - Onsite and/or remote training provided for the merchant's fraud team
  - Support availability and response time

Product Roadmaps

Product Management Lifecycle

A product management lifecycle is made up of the processes and decisions a product management team takes to lead, drive, and guide a product across the entire span of its evolution—from its very beginnings as a concept to its reinvention or discontinuation.

Generally, leading product strategy means pulling in expertise from a range of teams including design, engineering, finance, and marketing—to create, develop, and market the product. These teams work collaboratively with the project management team that ensures clear planning, organization, workflows, and delivery.

- ☑ **Lifecycle Phase 1: Ideation**
  A product life cycle involves lots of teams with the customer at the center of what they do—engineering, marketing, analytics, design—all with a perspective on customer pain points, possible solutions, and areas of opportunity.

- ☑ **Lifecycle Phase 2: Research and Development**
  At this stage, companies introduce their idea to target audience samples to gather quantitative and qualitative feedback to answer key questions, like what improvements can be made, and which of these would have the biggest impact.

- ☑ **Lifecycle Phase 3: Launch**
  An agile, iterative product management cycle depends on early market entry to start receiving and reacting to user feedback as quickly as possible—so the product at the time of launch must be a basic offering aimed at early adopters.

☑ **Lifecycle Phase 4: Feedback, Learn, and Respond**
With your MVP (Minimum Viable Product) launched, use ongoing user feedback to inform decision-making and continually shape and reshape the product for the user.

User Experience (UX) and Workflow Requirements

UX, which stands for "user experience." The term "user experience," refers to how people interact with a product. In the digital design world, UX refers to everything that affects a user's interaction with a digital product.

A UX workflow is a step-by-step process that designers follow from conceptualization to design handoff.

The following is a typical design workflow most UX teams use:

- Defining the business need
- Conducting research and gaining insights
- Analyze research and ideate
- Creating information architecture and user flows
- Prototyping
- Testing
- Design handoff

The UX design now plays a significant role in the way a customer moves through the transactional process. The clarity of language, instructions, success, and error messages all help the customer have a smooth and secure experience.

Sample Exam Questions

1. What does consortium data refer to?
   a. Data that is sorted alphabetically across sources
   b. Data that is provided by a single source
   c. Data that is grouped together from multiple sources

2. Access Device Fraud is the legal term referencing fraud from which of the following sources?
   a. Hacking
   b. Payment cards
   c. Breaking and entering

Answers: 1-c, 2-b

GLOSSARY

Account Holder – A person who owns the account attached to a credit or debit card.

Address Verification System (AVS) – A payment processing system comparison of the numerical portions of billing and shipping addresses with the addresses on file at the credit card-issuing bank.

Artificial Intelligence (AI) – Computer systems used to perform complex tasks in a way that is similar to how humans solve problems.

Authorized Transaction — A debit or credit card transaction for which a merchant receives authorization from the bank that issued the card. Also called card authorization, preauthorization, or preauth.

Cardholder – See "Account Holder."

Card Not Present (CNP) – A type of transaction in which neither the cardholder nor the credit card is physically present. It's most common for remote orders taken over the phone, by internet, or mail. These make up the bulk of eCommerce orders.

Card Verification Values (CVVs) – The three-to-four-digit security number found on the back of credit cards that can help reduce the risk of credit card fraud. These numbers are printed on the card, rather than embossed or stored in the magnetic strip.

Chargebacks - Credit card chargebacks occur when a customer disputes a transaction and asks the credit card issuer to reverse the charge.

Chargeback Ratio - The number of chargebacks compared to the overall transactions for a given month. As the number of chargebacks against a retailer rises, so does the ratio.

Credit Card Fraud – A form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it.

Dark Web - A part of the World Wide Web not accessed by traditional search engines like Google. Dark websites use a layered network structure to encrypt web traffic.

Data Breach – An incident in which sensitive, protected or confidential data (including financial information, health data, passwords, or credit card information) is accessed through unauthorized means.

Deep Learning – A type of machine learning technique that uses a multilayered approach to learning that lets human analysts feed data and a learning algorithm to a computer to allow the computer to teach itself to make decisions about that data.

Digital Wallet – Smartphone based payment tools like PayPal, Google Wallet, Amazon Wallet and Apple Pay that make it easier and faster for customers to make purchases online and at brick-and-mortar locations. Digital wallets use advanced encryption technology and passwords to protect against fraudulent use.

Dispute – Established through The Fair Credit Billing Act of 1975, a dispute is the act of a customer formally questioning and contesting transactions on their statements.

eCommerce - Electronic commerce transactions that occur through an electronic medium between businesses and consumers.

First-Party Misuse – See "Friendly Fraud."

Fraud – Wrongful or criminal deception intended to result in financial or personal gain.

Friendly Fraud - When a cardholder disputes a transaction for reasons not intended to be deceitful, like forgetting they made the purchase, not recognizing the merchant's name on their statement, or not knowing another family member authorized a purchase.

Fraud Prevention - The implementation of a strategy to detect fraudulent transactions and prevent these actions from causing financial and reputational damage to a merchant or customer.

Fraud Rate – Normally measured by chargebacks, fraud rate is a combination of gross chargebacks that the merchant receives, while net chargeback is everything the merchant receives minus every chargeback they dispute.

Identity Theft - When fraudsters use personal data such as an individual's name, driver's license number, date of birth and address, to pose as that person to open new accounts and make purchases.

Machine Learning (ML) - A subfield of artificial intelligence, ML is the capability of a machine to imitate intelligent human behavior. ML is frequently used with fraud software and human analysts to find fraud patterns in purchase data, make predictions, flag fraud, and make fast transactional decisions while minimizing risk exposure.

Merchant Account – a type of business bank account that allows a business to accept and process electronic payment card transactions.

Payment Authorization Rate – how many people are being approved when they attempt to purchase your product, and how many are being rejected. This metric is directly linked to revenue coming into a merchant's business.

Payment Card Industry (PCI) – PCI compliance is the set of technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.

Phishing – A form of social engineering and identity theft in which an e-mail user is tricked into revealing personal or confidential information which the scammer can use illicitly. Phishers may also install malicious software on computers, infect computers with viruses or even steal personal information off computers.

Point-to-Point Encryption – The PCI Security Standards Council established P2PE standards to improve the security of credit card transactions. During a P2PE process, transactional data is securely encrypted from point-of-sale entry to the final credit card processing point.

Ransomware – Malware used by cyber attackers to encrypt information and deny a user access to files on their own device until a ransom is paid for a decryption key to regain access to their files.

Risk Management – The process of identifying, assessing, and controlling threats to an organization's capital and earnings. Risks stem from a variety of sources including financial uncertainties, fraudulent behavior, legal liabilities, technology breaches, accidents, and natural disasters.

Risk Rejects – How many times is a merchant's risk service rejecting a customer because they suspect they are a fraudster. It is important to know if rejections are people committing fraud or if they are false positives (good customers being blocked), and how to measure and balance between the two.

Skimming - The act of using hidden electronic devices or card readers at point-of-sale systems to capture and copy electronically transmitted account information from a valid credit or debit card.

Transaction Optimization – To improve the performance of the synchronization point processing between transaction branches on the client side and the server side.

True Fraud – A malicious act in which a customer's identity or card is stolen and used for a purchase without their knowledge.

ADDITIONAL RESOURCES

Exam Content Outline

A. Performance Management
- ☑ Data analysis (e.g., descriptives, projections, artificial intelligence [AI], using data to draw insights for risk mitigation)
- ☑ Financial principles (e.g., return on investment [ROI])
- ☑ Global and regional payment protocols and data flows (e.g., ISO 8583)
- ☑ Data modeling (e.g., optimizing transaction routing decision)
- ☑ Fraud and payments KPIs (e.g., authorization rate, merchant fee, manual review rate)
- ☑ Payments performance benchmarks (e.g., digital versus physical, geography)
- ☑ Payments response codes (e.g., insufficient funds)
- ☑ Threat landscape (e.g., payment method with high probability of synthetic accounts, used in account takeover and payment fraud)
- ☑ Fraud management strategies
- ☑ Information security (e.g., phishing, social engineering, dark web, malware, ransomware)

B. Operational Management
- ☑ Payment processing requirements and regulations (e.g., card network mandates)
- ☑ Industry fraud patterns and best practices
- ☑ Chargeback representment strategies (e.g., success metrics [win rate], reason codes, compelling evidence rules)
- ☑ Fraud detection and prevention operations (e.g., techniques)
- ☑ Fraud prevention policies and controls
- ☑ Fraud patterns (e.g., trends versus patterns, business and industry, balancing customer experience against rising fraud threats)

C. Provider Management
- ☑ Service provider management
- ☑ Contract management
- ☑ Fees and fines (e.g., interchange, assessment fees, processing fees, foreign exchange rates, fraud threshold fines)
- ☑ Global and regional payment ecosystems and regulations impacting payments (e.g., payments processing, card acquirers, banking (risk department), or eCommerce platform, GDPR)

D. Features and Enhancements
- ☑ Architecture and flows between internal systems/services
- ☑ Global and regional payment methods and associated risks and tradeoffs
- ☑ Payments security and compliance (e.g., internal controls and audit procedures)

- ☑ Components of a contract (e.g., leveraging penalties, incentives, service requirements, payment costs)
- ☑ Technical and business requirements associated with product launching
- ☑ Product roadmaps
- ☑ Product management lifecycle and processes
- ☑ User experience (UX) and workflow requirements
- ☑ Fraud technologies internal and external

Books and Websites

This reference list contains journals, textbooks, and web sites that include information of significance to the CPFPP field. This list is subject to change and will be updated as new resources become available. Visit the CPFPP Exam page to see updated information.

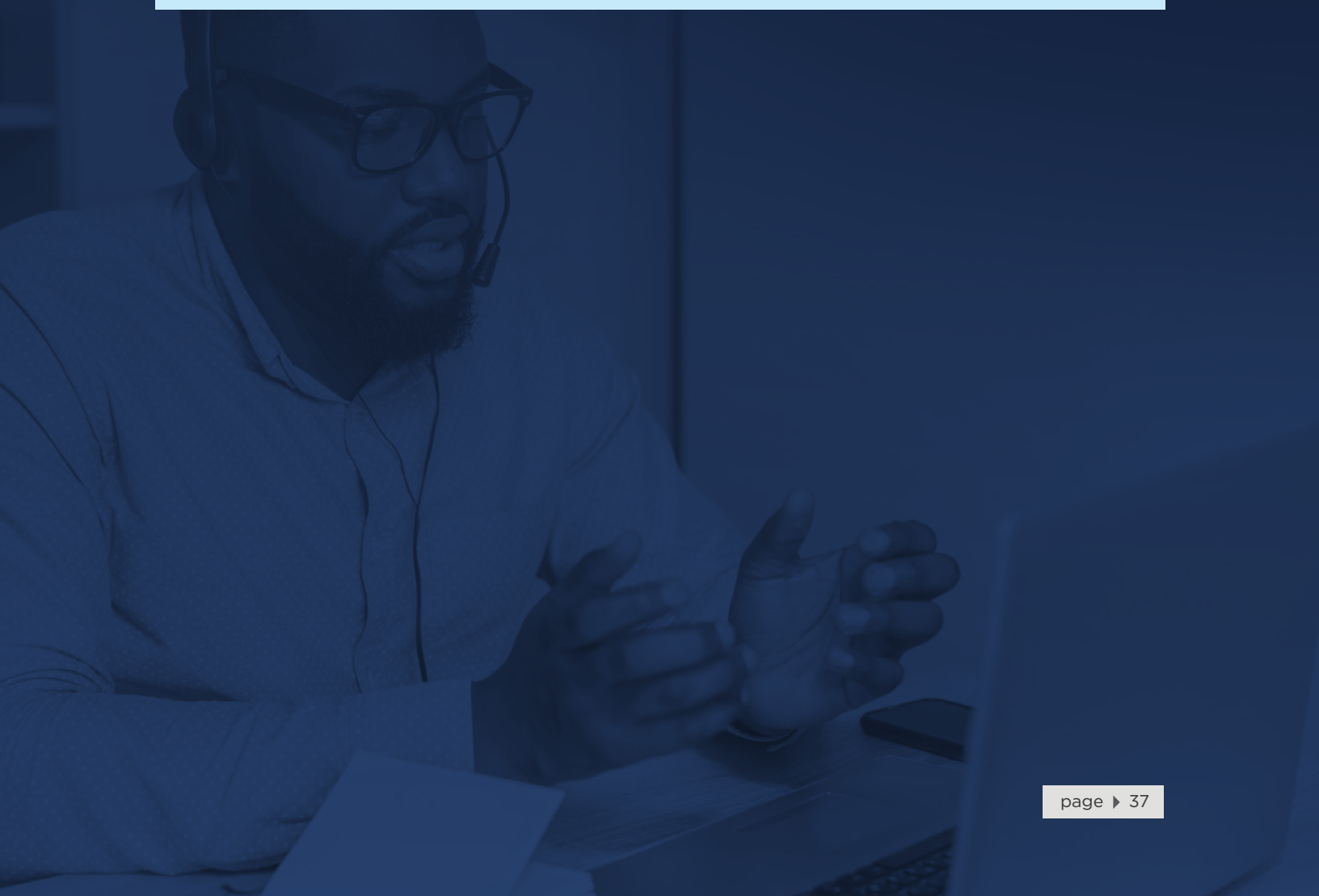
- 3DS Secure
- PCI Security Standards
- Glenbrook Payment Textbooks
- Visa Dispute Management
- Mastercard Chargebacks Guide
- MRC 2022 Global Payments and Fraud Survey Report
- MRC 2021 Global Fraud Survey Report
- MRC 2020 Global Payments Survey Report

[MRC How to Create a Fraud Prevention Unit]

[Practical Fraud Prevention]

[GDPR]

[American Express Merchant Operating Guide]



I've spent most of my career dealing with risk, fraud, and charge-backs while also dabbling in other areas of payments. I saw the CPFPP exam as a way to legitimize the experience and skills I've accumulated through an organization I respect and am regularly involved with.

Robert Rix, CPFPP
Fraud Program Manager, Trust and Safety
TaskRabbit

The CPFPP certification program highlights an evolving industry that is a revenue driver, cost mitigator, and essential part of any organization. I saw it as an opportunity to test myself, my knowledge, and enhance my development and scope in the payments landscape. Passing the exam distinguishes me and acknowledges my expertise in the payments and fraud landscape.

John Szczuplak, CPFPP, CTP
Senior Treasury Manager
L'ORÉAL USA

Contact Us

merchantriskcouncil.org

certification@merchantriskcouncil.org