# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Use This Study Guide</td>
<td>1</td>
</tr>
<tr>
<td>Study Strategies and Test Taking Tips</td>
<td>2</td>
</tr>
<tr>
<td>ETA CPP Examination</td>
<td>2</td>
</tr>
<tr>
<td>Study Plan Development</td>
<td>2</td>
</tr>
<tr>
<td>Study Strategies</td>
<td>2</td>
</tr>
<tr>
<td>Test Taking Tips</td>
<td>3</td>
</tr>
<tr>
<td><strong>Exam Question Format</strong></td>
<td>4</td>
</tr>
<tr>
<td>Common Types of Multiple-Choice Questions</td>
<td>4</td>
</tr>
<tr>
<td><strong>Exam Content Outline</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Overview of Test Specifications</strong></td>
<td>7</td>
</tr>
<tr>
<td>Domain 1: Sales</td>
<td>7</td>
</tr>
<tr>
<td>Domain 2: Pricing and Interchange</td>
<td>12</td>
</tr>
<tr>
<td>Domain 3: Process/Operations/Workflow</td>
<td>16</td>
</tr>
<tr>
<td>Domain 4: Products/Solutions/Mobile Technology</td>
<td>23</td>
</tr>
<tr>
<td>Domain 5: Risk</td>
<td>36</td>
</tr>
<tr>
<td>Domain 6: Regulatory/Compliance/Security</td>
<td>45</td>
</tr>
<tr>
<td><strong>Sample ETA CPP Examination Questions</strong></td>
<td>48</td>
</tr>
<tr>
<td>Sample Questions</td>
<td>48</td>
</tr>
<tr>
<td>Answer Key</td>
<td>57</td>
</tr>
<tr>
<td><strong>Reference Material and Additional Resources</strong></td>
<td>58</td>
</tr>
</tbody>
</table>
**HOW TO USE THIS STUDY GUIDE**

For complete and detailed information on the ETA CPP examination, please visit www.electran.org/cpp.

This study guide is designed to help you prepare for the ETA Certified Payments Professional (CPP) examination. The examination covers a broad overview of the electronic payments industry. This study guide provides a more in-depth overview of the topics covered on the examination, as well as suggested resources and reference material in the event you wish to dive deeper into certain topic areas.

It is NOT a definitive work on all of the elements within the test, nor is it a listing of the minimum required reading necessary to pass the exam. There are no exam eligibility requirements other than work experience. This study guide is not a replacement for active industry study, on-the-job training, and learning from other sources within the payments industry.

The ETA CPP examination has been developed in collaboration with Castle Worldwide of Raleigh, NC.

---

**Testing Windows**

The examination is offered in two 30-day testing windows.

<table>
<thead>
<tr>
<th>Testing Windows</th>
<th>Application Deadline*</th>
<th>Cancellation/ Rescheduling Request Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 1 – 30</td>
<td>May 1</td>
<td>No later than 4 business days prior to your testing appointment</td>
</tr>
<tr>
<td>December 1 – 31</td>
<td>November 1</td>
<td></td>
</tr>
</tbody>
</table>

*Applications received after the final postmark deadline will automatically be deferred to the next available testing window.
The following strategies and test taking tips are provided to help you prepare for the ETA CPP exam. However, we encourage you to seek other independent resources, some of which are listed throughout this study guide, to obtain a more thorough overview of specific topic areas.

Please refer to the Candidate Handbook on the ETA website (www.electran.org/cpp) for important information on scheduling your exam and what to expect once you arrive at the test center. Regardless of how well you prepare for the exam, your efforts will go unrewarded if you do not fully comply with the exam scheduling and test center admission requirements.

The Electronic Transactions Association (ETA) wishes you the best in your efforts to prepare for the exam and looks forward to adding your name to the registry of ETA Certified Payments Professionals™.

ETA CPP Examination

The ETA CPP examination is made up of 125 multiple-choice questions and is based on the concepts and experiences germane to the electronic transactions industry. The topics are derived from the Test Content Outline, based on the Job Task Analysis survey of industry practitioners, administered on a regular basis. The test content areas and specifications are listed below:

2016 – 2018 ETA CPP Test Specifications

<table>
<thead>
<tr>
<th>Area</th>
<th>Percent of Exam</th>
<th>Number of Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain 1: Sales</td>
<td>18%</td>
<td>22</td>
</tr>
<tr>
<td>Domain 2: Pricing and Interchange</td>
<td>17%</td>
<td>21</td>
</tr>
<tr>
<td>Domain 3: Process/Operations/Workflow</td>
<td>15%</td>
<td>19</td>
</tr>
<tr>
<td>Domain 4: Products/Solutions/Mobile Technology</td>
<td>15%</td>
<td>19</td>
</tr>
<tr>
<td>Domain 5: Risk</td>
<td>19%</td>
<td>24</td>
</tr>
<tr>
<td>Domain 6: Regulatory/Compliance/Security</td>
<td>16%</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>125</td>
</tr>
</tbody>
</table>

Note: The questions in each content area are distributed randomly throughout the examination.

The exam is computer based and is administered at approximately 1,000 proctored test center locations in over 700 cities in over 70 countries around the world. All testing center personnel follow standard testing industry protocol when administering the exams, so it is in your best interest to understand and follow the testing policies, procedures and guidelines to ensure a positive testing experience.

Your total seat time at the testing center is three hours. Please ensure you read and understand everything listed on the computer screen before you begin the examination.

Recommended Study Plan Development

- Allow a sufficient period for studying. Review the entire test content outline to determine how familiar you are with the content of the exam.
- The ETA CPP examination is based upon the test content outline, but the test questions are written to general practice and are not specific to any one organization’s practices or policies.
- Identify your “knowledge gaps.” This means that you need to identify what you do NOT know. While a thorough review of the exam content is beneficial, you will need to devote extra attention to areas that are less familiar to you.

Recommended Study Strategies

- Determine a study location that will allow you uninterrupted study periods.
- Create flash cards or recordings to review exam material. This will reinforce your learning.
- Arrange your study time by the number of test questions from each content area (see chart this page) and the amount of information you already know.
- Develop and share test questions with other candidates to challenge your knowledge. This will help you “drill down” into the material and acquire a greater understanding of some concepts.
- Try to closely simulate an exam experience. We encourage candidates to try to test in half the time. By doing so, you will allow yourself enough time to go back and review questions you may have skipped or marked for review.
Test Taking Tips

- If you are unsure about how to use the computer, or if you have any questions about the procedures for the exam, ask the testing center personnel before the exam begins.
- Programmable calculators, phones and PDAs are not allowed. An on-screen calculator similar to those available on all PCs will be provided on the testing computer, if needed.
- Each question on the examination contains only one correct answer and three incorrect options.
- There is no penalty for incorrect answers, so plan to answer every question. You are not penalized for guessing. In the multiple-choice question of four answer options, you stand a 25% chance of guessing correctly.
- The ETA CPP exam contains 125 questions, which you need to answer within 3 hours. That means you have just over a minute and a half per question, on average. But you should really try to make your first pass through all the questions in 75 minutes. That way, you will move quickly through easy-to-answer questions and save yourself plenty of time to return to the harder questions.
- Answer questions that are obvious to you first. Mark difficult questions to come back to later. Every question is worth the same number of points. Make your best selection and/or mark it for later review and move on to the next question.
- Do not go too fast or skim through the questions or answers. You may end up making careless mistakes.
- Read the entire question and all answer options carefully before making your selection.
- Do not overanalyze or try to “read into” a question. Questions are not written to be tricky. Do not assume additional information beyond what is given in the test question. All information necessary to answer the question will be given in the text of the question or scenario.
- If there are questions including the words “not,” “except,” or “least,” answer with particular care because you will be looking for the exception. These questions involve a reversal of your usual thought patterns.
- Pay close attention to key words such as “best,” “most,” “primary,” or “usually.” These words indicate that other options may at times be correct, but given the wording or situation in the test question, you must judge which option is the best.
- Let your original answer stand unless you are completely sure about the new answer.
- Do not let your work experience dictate how you answer a question. The exam is based upon an accepted knowledge base as outlined in the ETA CPP Test Content Outline. Choose options that you know to be correct in any setting, not just your place of employment.
- Ignore other test takers. Their anxiety can be contagious.
- Relax the night before the test and get a good night’s sleep. You have prepared well in advance, so the night before the test is time to relax.
- Make sure you know exactly where the test center is located. If possible, drive to the test center the day before the exam. Be sure to leave yourself plenty of time to get there on exam day.
Common Types of Multiple-Choice Questions

The following are samples of the types of question formats which may be used on the ETA CPP examination:

1. Closed question
   - A complete question followed by four (4) optional answers, only one of which is correct. Often, the word “what” is included in the question.
   Example: What is the usual color for stop signs?
   a. Red
   b. Yellow
   c. Green
   d. Purple
   - A complete question that includes the phrase “which of the following” when there is more than one correct answer to a question, but only one of the correct answers is offered in the options.
   Example: Which of the following colors is a combination of two primary colors?
   a. Red
   b. Purple
   c. Yellow
   d. Blue

2. Open question
   - An incomplete sentence with four (4) optional completions, only ONE of which is correct.
   Example: A period of time of 60 minutes is called a(n):
   a. Hour
   b. Week
   c. Month
   d. Year

3. Exception
   - A format used when three (3) of the options are correct and only one option is incorrect. The incorrect option is actually the correct answer in this case.
   Example: All of the following statements about ice cream are true EXCEPT:
   a. It should be stored in the freezer.
   b. It has very few calories.
   c. It comes in many flavors.
   d. It is a popular snack food.

4. Item Sets
   - A set of questions based on information contained in the preceding paragraph.
   Example: Questions 1 and 2 are based on the following information: There are 365 days in a year, 7 days in a week and 12 months in a year.
   1. How many weeks are there in a year?
      a. 50
      b. 52
      c. 54
      d. 55.14
   2. What is the average number of days in a month?
      a. 29.5
      b. 30
      c. 30.42
      d. 32.39
EXAM CONTENT OUTLINE

Domain 1: Sales

Task 1: Identify prospective merchant customers by following corporate-standard lead generation procedures to ensure a continuous pipeline of potential customers.

Task 2: Prioritize prospective merchants based on company guidelines and weighted revenue potential to maximize revenue results.

Task 3: Contact prospects and, through relationship building techniques, locate decision-makers to solicit business.

Task 4: Recommend appropriate products and solutions to merchants through consultative communication of product/solution capabilities.

Task 5: Identify and understand the merchant’s needs and goals, through information gathered from the merchant and other research in order to meet the merchant’s objectives.

Task 6: Present appropriate solutions to the merchant decision-maker based on needs and goals identified in order to help the merchant make the purchase decision using verbal and written presentation skills and other available resources.

Task 7: Listen to and understand merchant objections so they can be overcome, and make the sale by presenting the appropriate information and solutions.

Task 8: Negotiate pricing terms with merchant in order to establish a mutually beneficial long-term relationship for both parties to successfully complete the business transaction.

Task 9: Execute the contract with the merchant through corporate standard procedures in order to realize the sale.

Task 10: Implement all corporate-standard contract completion procedures to include contract signatures, contract receipt confirmation, merchant delivery and installation scheduling, and customer post-sale follow-up in order to ensure customer satisfaction and ongoing upsells and referrals.

Task 11: Provide ongoing, timely response to merchant needs through prompt response to issues and proactive support to ensure satisfaction and retention.

Task 12: Maintain client database in order to keep track of current sales channel information to avoid multiple sales solicitations, communicate sales status, retain contact information, and maintain efficiency.

Task 13: Maintain industry knowledge (techniques, new tactics, etc.) and proficiency, and ensure continued client satisfaction by regularly attending continuing education programs, according to standard corporate policy.

Task 14: Acquire in-depth understanding of contract terms and conditions in order to ensure legal execution of contract and protection of all stakeholders.

Domain 2: Pricing and Interchange

Task 1: Acquire and maintain current knowledge of all interchange categories and all other fees by reviewing materials provided by Acquirers, Card Brands, and Processor to educate merchants and maintain profitability of the portfolio.

Task 2: Analyze competitors’ merchant processing statements in order to compare those statements with your own pricing plans.

Task 3: Analyze prospective customer’s current merchant processing statements for rate comparison to efficiently determine if the profitability objectives of all parties can be met.

Task 4: Acquire up-to-date information on all ancillary product opportunities to be able to recommend appropriate products and pricing that meet the merchant’s business needs.

Task 5: Provide market feedback of competitor pricing to corporate to identify needed pricing adjustments and new revenue streams using communication with merchants and other channels.
## EXAM CONTENT OUTLINE

### Domain 3: Process / Operations / Workflow

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Acquire in-depth understanding of complete workflow from contract signing, boarding, approval, through live MID in order to ensure that merchant is approved and begins processing transactions.</td>
</tr>
<tr>
<td>2</td>
<td>Acquire in-depth understanding of ongoing support processes in order to successfully retain merchants and generate new revenue through up-sell opportunities and referrals.</td>
</tr>
<tr>
<td>3</td>
<td>Acquire in-depth knowledge of all participants, components, and stakeholders associated with completing a payment transaction in order to be able to explain these same issues to stakeholders.</td>
</tr>
</tbody>
</table>

### Domain 4: Products, Solutions, and Mobile Technology

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ask merchant-specific qualifying questions in order to evaluate and ultimately meet or exceed merchant-specific needs.</td>
</tr>
<tr>
<td>2</td>
<td>Determine the optimal solution from all available product configurations to satisfy or surpass the merchant’s needs.</td>
</tr>
<tr>
<td>3</td>
<td>Test and train the merchant on new solutions, whether installed by a third party or employer, to ensure a fully prepared, educated, and active merchant.</td>
</tr>
<tr>
<td>4</td>
<td>Demonstrate a complete understanding of challenges, issues, requirements, and opportunities when troubleshooting maintenance situations.</td>
</tr>
<tr>
<td>5</td>
<td>Demonstrate a broad understanding of technologies and products within the payment processing industry to meet current and future regulatory requirements.</td>
</tr>
<tr>
<td>6</td>
<td>Demonstrate a broad understanding of technologies and products for new and emerging technologies, most notably EuroPay MasterCard Visa (EMV)</td>
</tr>
<tr>
<td>7</td>
<td>Demonstrate a broad understanding of technologies and products for new and emerging technologies, most notably Near Field Communication (NFC)</td>
</tr>
<tr>
<td>8</td>
<td>Demonstrate a broad understanding of technologies and products for new and emerging technologies, most notably Mobile payments</td>
</tr>
</tbody>
</table>

### Domain 5: Risk

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Evaluate specific merchant characteristics regarding how the merchant conducts business to determine merchant fit with corporate and industry specific guidelines.</td>
</tr>
<tr>
<td>2</td>
<td>Compare merchant actual results against application assumptions to retain merchant and prevent losses.</td>
</tr>
<tr>
<td>3</td>
<td>Educate merchant by applying industry best practices of card acceptance in order to prevent consumer fraud and chargebacks (collected or uncollected).</td>
</tr>
<tr>
<td>4</td>
<td>Maintain broad understanding and knowledge of your individual acquirer, and general knowledge of your corporate risk policy and the industry’s critical factors to balance fiscal success against potential losses.</td>
</tr>
</tbody>
</table>

### Domain 6: Regulatory / Compliance / Security

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Acquire and maintain current knowledge of appropriate and available regulations governing the payment processing industry through trade organizations, card brands, media, networking, magazines, online resources, etc. in order to educate merchants and ensure compliance by the sales agent, consumer, and merchant.</td>
</tr>
<tr>
<td>2</td>
<td>Educate merchant base on all applicable regulations, compliance, and the impact of non-compliance by presenting merchants with verbal and written materials to avoid sanctions and fines.</td>
</tr>
<tr>
<td>3</td>
<td>Gather proper documentation from merchant to make sure merchants are compliant with all regulations.</td>
</tr>
<tr>
<td>4</td>
<td>Inform merchants of all data management, security, and storage regulations and best practices to ensure compliance by all stakeholders.</td>
</tr>
</tbody>
</table>
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 1

DOMAIN 1: SALES

Task 1: Identify prospective merchant customers by following corporate-standard lead generation procedures to ensure a continuous pipeline of potential customers.

Objectives
This task requires that a certified payments professional be able to:
- Understand the various lead sources available within their organizations, whether the source comes from marketing or within the sales organization;
- Develop a cohesive plan of action with regard to cold calling target merchant markets;
- Understand how to build referral partner relationships;
- Have the ability to organize and maintain detailed lists of information to track and maintain pipeline;
- Understand and manage diverse lead sources based on industry, geography, market niche, expertise, local business drivers and corporate requirements.
- Follow up with potential and current customers; and
- Written and oral communication skills.

Task 2: Prioritize prospective merchants based on company guidelines and weighted revenue potential to maximize revenue results.

Objectives
This task requires that a certified payments professional be able to:
- Identify the target market(s) and vertical(s) based on corporate standards and personal experience and expertise;
- Prioritize high value merchant prospects based on size and potential; and
- Manage pipeline of contacts and business opportunities within defined corporate guidelines; and
- Organizing and maintaining detailed lists of information.

Task 3: Contact prospects and, through relationship building techniques, locate decision-makers to solicit business.

Objectives
This task requires that a certified payments professional be able to:
- Understand how merchant businesses are structured and who makes the buying decisions;
- Understand “active listening;” “Ask, Listen, Solve;”
- Understand the different type of questions to ask: confirming, open ended, or clarifying;
- Identify decision maker; and
- Prioritizing potential customers/prospects.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 1

Task 4: Recommend appropriate products and solutions to merchants through consultative communication of product/solution capabilities.

Objectives
This task requires that a certified payments professional be able to:
- Understand the “consultative sales approach” and the effective use of questioning and understanding customer needs;
- Understand products, solutions and technologies offered by your organization; as well as your competitors;
- Learn highly technical product/service offerings; and
- Utilizing VAR sheets and lists of compliant products to select preferred offering.

Task 5: Identify and understand the merchant’s needs and goals, through information gathered from the merchant and other research in order to meet the merchant objectives.

Objectives
This task requires that a certified payments professional be able to:
- Demonstrate knowledge of consultative sales techniques, strategies and practices;
- Perform a needs analysis to ensure appropriate understanding of the merchant’s business and their goals and objectives for the business...;
- Understand how to perform “active” listening and apply the information both spoken and inferred by the client into needs and opportunities;
- Value-added sales propositions vs. commodity sales; and
- Communicate complex technical concepts to highly varied audiences.

Task 6: Present appropriate solutions to the merchant decision maker based on needs and goals identified in order to help the merchant make the purchase decision using verbal and written presentation skills and other available resources.

Objectives
This task requires that a certified payments professional be able to:
- Demonstrate knowledge of competitive products, solutions and technologies;
- Demonstrate proficiency in presentation skills utilizing “feature, advantage, benefit analysis;” and
- Understand the necessary criteria and requirements to communicate an effective offer and meet the needs of management and legal requirements.
- Written and verbal communications;
- Demonstrating complex technological solutions; and
- Applying product knowledge to highly varied application requirements.
Task 7: Listen to and understand merchant objections so you can overcome them, and make the sale by presenting the appropriate information and solutions.

**Objectives**
This task requires that a certified payments professional be able to:
- Formulate/implement probing questions as you work with merchant prospects;
- Understand a prospect’s primary objections and the driving factors to those objections; and
- Objection handling techniques;
- Knowledge of features and benefits difference;
- Value-added sales concepts; and
- Closing techniques.

Task 8: Negotiate pricing terms with merchant in order to establish a mutually beneficial long-term relationship for both parties to successfully complete the business transaction.

**Objectives**
This task requires that a certified payments professional be able to:
- Understand and communicate all applicable pricing terms and conditions;
- Demonstrate the necessary regulatory requirements for pricing and answers for pricing related questions;
- Sell value over price;
- Understand the correct pricing structure for the merchants in order to solve any billing issues they may have with their current processor;
- Win-Win negotiation strategies techniques;
- Active listening; and
- Closing techniques.

Task 9: Execute the contract with the merchant through corporate standard procedures in order to realize the sale.

**Objectives**
This task requires that a certified payments professional be able to:
- Obtain all legal requirements and/or corporate documentation to execute the agreement;
- Demonstrate knowledge of the processes and steps to submit a properly executed agreement that meets the needs of the corporation and of the card brands;
- Formulating and implementing probing questions;
- Active listening.
Task 10: Implement all corporate-standard contract completion procedures to include contract signatures, contract receipt confirmation, merchant delivery and installation scheduling, and customer post-sale follow-up in order to ensure customer satisfaction and ongoing upsells and referrals.

Objectives
This task requires that a certified payments professional be able to:

- Understand all of the corporate and regulatory information required to obtain approval;
- Understand the rights and requirements of the client in completing an application;
- Demonstrate knowledge of “post signup” installation requirements and processes necessary to fully finalize a client implementation;
- Obtain required information;
- Organizing and follow up on information; and
- Written and verbal communication

Task 11: Provide ongoing, timely response to merchant needs through prompt response to issues and proactive support to ensure satisfaction and retention.

Objectives
On completion of this task, certified payments professionals should be able to:

- Demonstrate knowledge of managing merchant expectations;
- Understand the corporate needs and requirements of local access and respond to client needs;
- Leave merchant with all appropriate service numbers for technical inquiries, service inquiries, and escalation…;
- Documenting and communicating effective corrective solutions to employer and corporate.

Task 12: Maintain client database in order to keep track of current sales channel information to avoid multiple sales solicitations, communicate sales status, retain contact information, and maintain efficiency.

Objectives
This task requires that a certified payments professional be able to:

- Understand and leverage your organization’s CRM solutions to track your merchant database;
- Demonstrate the ability to input, track and effectively manage customer contact and follow up using SFA and CRM applications; and
- Develop a follow up plan and a set of objectives to enhance one’s ability to move the prospect quickly through the various sales processes.
- Creating reports of sales activity;
- Forecasting; and
- Building, maintaining, and managing lists of complex information.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 1

Task 13: Maintain industry knowledge (techniques, new tactics, etc.) and proficiency, and ensure continued client satisfaction by regularly attending continuing education programs, according to standard corporate policy.

Objectives
This task requires that a certified payments professional be able to:
- Demonstrate knowledge of current and future payment industry trends; and
- Understand the sources and resources available to agents in maintaining proficiency in the industry;
- Sourcing and integrating large amounts of diverse information; and
- Applying newly acquired information into day-to-day activities.

Task 14: Acquire in-depth understanding of contract terms and conditions in order to ensure legal execution of contract and protection of all stakeholders.

Objectives
This task requires that a certified payments professional be able to:
- Understand and communicate applicable laws, regulations and rules impacting the payments industry as required by the company, mandated by the card brands, and as applicable to individual merchant needs based on the processing process they use; and
- Demonstrate a working knowledge of the structure of the industry and the resources available to resolve and manage information and requirements based on industry updates and changes;
- Sourcing and integrating large amounts of diverse information;
- Applying newly acquired information into day-to-day activities; and
- Communicating potential threats and issues to all contract parties.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 2

DOMAIN 2: Pricing and Interchange

Task 1: Acquire and maintain current knowledge of all interchange categories and all other fees by reviewing materials provided by acquirers/card brands/processors in order to educate merchants and maintain profitability of the portfolio.

Objectives

This task requires that a certified payments professional be able to:

- Understand what interchange is and how it works; and
- Understand the merchant benefits for accepting credit/debit cards.

Understand the myriad of Interchange categories such as:

How Interchange Works

- Understanding what interchange is and how it works, specifically an understanding of the flow of interchange between the acquiring and issuing partners in the payments process, is critical to ensuring your merchants are priced appropriately and are provided with the appropriate products to qualify for the targeted interchange rates. However, interchange is only one component of the fees assessed to merchants. It is just as important to understand the various other fees and assessments that exist in addition to the interchange assessed on transactions. Many are from the card brands, others are part of the service offerings from the payments processors or the acquirer. Your understanding should include, but not be limited to the following fees:
  - Card brand dues and assessments
  - NABU, APF and FANF
  - AVS and switch fees
  - Authorization, batch and terminal related fees
  - Clearing and settlement fees
  - Customer service and support fees for POS, for back office
  - Chargeback and representment fees
  - PCI, statement or reporting fees
  - Sponsorship fees

Merchant Benefits of Card Acceptance

- The benefits of card payment acceptance are numerous and vary based upon the industry in which your merchant operates. Benefits of card acceptance for a B2B merchant will differ from those for a high volume quick service restaurant. An e-commerce merchant will benefit differently than a plumber operating out in the field. You should be able to articulate the benefits of the various card types (PIN debit, signature debit, prepaid, purchasing card, etc.) in a manner specific to your merchant’s needs. Further, many additional benefits of card acceptance exist in the technologies and methods you will recommend or sell to your merchant. These all work together as part of the payments process and should be understood as such.

Interchange Categories

- Along with understanding the interchange categories, it is important to be able to explain how and when your merchant may encounter transactions qualifying for each of the rates. It used to be as simple as card swipe rates and non-swipe rates. Today, it depends on the card type, the data passed along from the POS, the programs in place by the issuer and other ancillary data that moves through the systems with each transaction. While it is not necessary to know all the details, it is necessary to understand the qualification requirements for these interchange categories and appropriately convey these requirements to merchants.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 2

Credit/Debit/Prepaid
- Consumer/Commercial
- Rewards Cards
- Card Present/Card Not Present transactions
- Regulated/Non-Regulated
- No Signature Required
- Quick Service Restaurants (QSR)
- Supermarket
- Fuel
- Small Ticket
- Emerging Markets
- Level 1, 2 and 3 Data

Task 2: Analyze competitors’ merchant processing statements in order to compare those statements with your own pricing plans.

Objectives
This task requires that a certified payments professional be able to:
- Know what to look for when reviewing a merchant’s monthly processing statement, including items such as:

Analyzing Merchant Processing Statements
Merchant statements are produced in any number of formats, making analysis of a merchant statement as much an art as a necessary skill. In general, a competency in identifying the following items and how they correlate to costs and profits serve as a base requirement in statement analysis. You should understand and be able to convey the definition or meanings of these along with others that may be less typical on a merchant statement.

- Discount Rate (Credit/Debit)
- Cost Plus
- Daily or monthly discount
- Surcharge/Billback/ERR Rates
- Sales Volume/Transaction Counts
- Average Ticket
- Settled vs. Non-Settled
- % Credit vs. % Debit
- Authorization Fees
- Statement Fees, Annual Fees, Other Misc. Fees
- Effective Rate
- Third party services such as check or gift
- Batches
- Deposits
- Chargeback Activity
- PCI Compliance/Non-Compliance
- Regulatory Product Fees
Task 3: Analyze prospective customers’ current merchant processing statements for rate comparison to efficiently determine if the profitability objectives of all parties can be met.

**Objectives**

This task requires that a certified payments professional be able to:

- Recognize industry pricing methodologies and utilize knowledge to prepare price quotes for merchants based on information on the statement; and
- Convert miscellaneous fees into basis points and vice versa.

**Industry Pricing Methodologies**

There are many pricing methodologies employed in the industry today. These can vary from tiered pricing and cost-plus (often referred to as interchange plus) to ERR or Billback pricing methods. Any of these methods may provide advantages to the merchant and to the acquirer and are often deployed on a merchant by merchant basis. A payments professional should be able to determine rather quickly what pricing method is being utilized on the merchant’s statement, and be able to easily suggest and explain why a particular pricing method may be better for that particular merchant. An understanding of qualified, non-qualified, mid-qualified, rewards, or discount rates and what downgrades mean from a pricing perspective is important. It is important to understand how a statement format that is different from your processor correlates to the statement presented by the merchant in order to ensure proposed pricing is accurately conveyed to the merchant.

Along with the interchange pricing, the acquirer has the option of bundling all the various fees or listing them a la carte or as line items on the statement. Obviously, if the statement you are viewing is a la carte AND cost plus, your job is much easier, as you can compare line items against your billing items. When a statement has bundled pricing, it is important to consider your “all-in” costs in a bundled fashion against the merchant statement presented, even if you intend to move the merchant to an unbundled program.

Task 4: Acquire up-to-date information on all ancillary product opportunities to be able to recommend appropriate products and pricing that meet the merchant’s business needs.

**Objectives**

This task requires that a certified payments professional be able to:

- Understand and explain the benefits of the different devices and Value Added Resources (VARs) to help assist merchants in processing transactions more efficiently. VAR stands for Value Added Reseller. The role of the VARs is to provide secure solutions that support and deliver the features you want your platform to offer.

Features facilitated by VARs include:

- Wireless and WiFi POS
- Internet Gateways
- Virtual Terminals
- Integrated POS system
- Dial-up POS terminals
- IP POS terminals
- Equipment Leasing options
- Multi-currency Options
- Gift and/or Loyalty cards
- Check conversion
- Cash advances
- ACH
These features may be among those requested by the merchant as a way to increase the service they can offer to their customers, to make the transaction process compatible with their overall business process, and to increase efficiency. All of this can solidify the merchant relationship and increase merchant retention. Some of these VAR features add steps to the entire process. However, if there is a problem with a VAR in the processing of a transaction the support staff will know instantly because the merchant will not be able to access the frontend system to get an authorization.

### Products and Pricing

Domain 4 covers products and services available or required for merchant payments processing and how they relate to the payments professional. For this domain, it is important to understand, address and convey a cost benefit analysis of a recommended payments solution, given a particular merchant’s payments processing needs. For example, if a merchant such as a plumber is processing a few thousand dollars a month and is simply entering card numbers into an Interactive Voice response system (IVR) from his phone for approval, the savings of swiping through a device attached to his mobile handset may not offset the cost of purchasing the device, the additional gateway fees or the monthly service fees.

At the same time, the plumber may find that efficiencies in reporting or speed of transaction processing are worth the few additional dollars for the service offering. Any discussion of products and services should include a consideration of the cost savings associated with interchange along with cost savings in time and resources. Both the hard and soft costs provide meaningful value to the merchant and can be addressed together or independently. Along with the cost savings in transaction processing, a payments professional should be able to accurately convey the costs associated with the service offering, including monthly fees, transaction fees, setup fees and other ongoing or occasional fees that may affect the overall cost of the service offering. The ability to understand the entire picture not only enables a payments professional to offer a better processing solution, but build a better merchant relationship.

### Task 5: Through communication with merchants and/or other channels, provide market feedback of competitor pricing to corporate to identify needed pricing adjustments and/or new revenue streams.

#### Objectives

This task requires that a certified payments professional be able to:

- Accurately spot pricing nuances on statements that identify new revenue streams, different ways to name or price items and differentiate between market “noise” vs. opportunity.

#### Pricing Nuances and Revenue Streams

An important component of being successful in the payments business is being able to sift through the “noise” from the merchant, your organization and the market. Staying abreast of market developments by reading card industry trade magazines, blogs, RSS feeds and websites is almost a must-do for any payments professional. Further, depending on your vertical market strategy, you should utilize similar resources in order to understand the environment in which your merchant operates and how you can correlate the other needs to the payment space.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 3

DOMAIN 3: PROCESS/OPERATIONS/WORKFLOW

Task 1: Acquire in-depth understanding of complete workflow from contract signing, boarding approval, through live MID in order to ensure that merchant is approved and begins processing transactions.

Objectives

This task requires that a certified payments professional be able to:

- Accurately and completely collect all necessary information and documentation as delineated in corporate policy;
- Understand application processing and the approval guidelines and communicate these guidelines to the merchant clearly and professionally when necessary; and
- Explain deployment of different terminal types and standard terminal functions.

Collect merchant application information

Each acquirer will have their own merchant application paperwork customized to their company. The following information must be provided on the merchant application:

- Business information – business name (DBA), physical location address, business telephone number and Tax Identification Number (TIN)/ Employer Identification Number (EIN).
- Contact information – Owner’s or Principal’s name and home address, alternate phone number, date of birth (DOB), and social security number, as a credit report will be obtained.
- Copy of the merchant’s voided check or bank letter with account name, account number and routing number, and a bank contact name and phone. Most processors will not allow “starter” or non pre-printed checks to be used.
- Cardholder Storage and PCI DSS – Questions on application must be completed entirely.
- A site survey is required to verify the physical location address belonging to the business name provided. A business license, fictitious business name filing (DBA), seller’s permit, and articles of incorporation or tax privilege license may be submitted to satisfy the site survey requirements.
- A personal guarantor for a merchant account may also be required. A personal guarantor ensures the full and faithful performance and payment responsibilities of the merchant to the acquirer and member bank, as outlined in the terms and conditions of the merchant processing agreement.

Upon receipt of the completed and signed application, the underwriting department will begin the review of the application. The average timeframe for approval is 24-48 hours. Once the application has been approved, the merchant may be provided with a merchant identification number, a welcome kit, a terminal, and terminal identification number if necessary.

Application processing and approval guidelines:

Application processing is the review, interpretation and entry of data appearing on a contract into a database for the purpose of obtaining an unsecured line of credit. This begins when a merchant completes and signs the contract.

Approval Guidelines

Standard types of merchant accounts:

- Retail – the selling of goods directly to the customer; face-to-face transaction
- Restaurant – an eating establishment where food and drink are being sold to customers
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 3

- Mail Order/Telephone Order (MOTO) or Internet – the selling of goods online; non-face-to-face transaction (ANY Card Not Present environment)
- Supermarket – large self-service retail store selling food and household goods
- Lodging – sleeping accommodations, furnished rooms to rent for the night

ISOs and MSPs will do their best to qualify a merchant for a merchant account. Statistically over 95% of applications received are approved. However, a few applications may be declined due to the business being against the member bank’s credit/risk policy, i.e., adult content, drug paraphernalia, gambling and lotteries. Restricted types of businesses may require additional documentation or information prior to approval, per card brand rules.

Deployment and standard terminal functions

Deployment providers may manage initial download of an acquirer’s application, prepare, test, package and ship a terminal to the merchant, and provide implementation services to merchant for system setup as well as repair and replacement services.

The different types of processing solutions are:

- Landline terminal – the card is swiped through a magnetic strip on the terminal, which connects to the processor’s computer.
  - Dial UP Terminal – A terminal that can read the track data on a magnetic stripe and communicate transaction information to the frontend platform and receives authorization instructions via the merchant’s phone line usually by dialing a toll free number.
  - IP Terminal - does the same thing as a dial terminal except that the terminal communicates transaction information to the frontend platform and receives authorization instructions by utilizing the merchant’s connection to the internet.
  - EMV Terminal has the ability to take cardholder data from a chip embedded within the card and communicate transaction information to the frontend platform and receives authorization instructions by utilizing the merchant’s phone line or Internet connection.

- Wireless terminal – provides the ideal solution for businesses seeking the most effective way to complete credit card transactions off-site. Most wireless credit card terminals support credit and debit transactions and are equipped with an internal PIN pad. Wireless terminals can be used on the countertop or in a mobile environment.

- Mobile solution – allows a merchant to accept credit cards using a cell phone with or without a card swipe mechanism.

- Internet solution – a processing method using a secure web server that provides an interface for merchant websites and shopping carts that require real-time transaction processing. Depending on the merchant’s software they can connect to a frontend via either an SSL server or payment gateway to get a real-time credit card authorization.

In addition, a peripheral device can be provided with a credit card terminal. Peripheral devices include:

- PIN pad – an electronic device used in a debit or smart card-based transaction to input and encrypt the cardholder’s PIN (personal identification number). The PIN pad is required so that the customer’s card can be accessed and the PIN can be securely entered and encrypted before it is sent to the transaction manager of the switch or the bank.

- Printer

- Check reader – a payment automation device that reads the MICR (Magnetic Ink Character Recognition) information on checks.

- Contactless reader – any pocket-sized card with embedded integrated circuits that can process and store data and communicate with a terminal via radio waves.

A few common warnings apply for most terminals when connecting the terminal to power. Do not use an adapter, power extender or an AC outlet that does not have ground connection. The AC adapter was designed for indoor use only; do not expose to rain or snow and do not immerse in fluid.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 3

Standard terminal functions include the following: sale, void last sale, and credit refund.

- **Sale** – for a sale, swipe the customer card or manually enter the credit card number, input sale amount, then press enter. The terminal will then transmit information through the network for approval, and a merchant receipt will be printed.
- **Void Last Sale** – to void the last sale, press the screen button next to void, choose last, verify transaction information on the display screen, then press enter. The transaction will be voided and a receipt showing the void will be printed.
- **Credit / refund** – to credit a refund, press the screen button next to refund, swipe the customer card, input return amount, press enter, and print merchant receipt.

*Many organizations do not allow refunds to be processed on PIN debit or EBT transactions. For signature debit, process a refund to the signature debit card used for the original purchase. For PIN debit, a cash refund or store credit must be given. For EBT, contact your state EBT office for a customer refund.*

**Task 2: Acquire in-depth understanding of ongoing support processes in order to successfully retain merchants and generate new revenue through upsell opportunities and referrals.**

**Objectives**

This task requires that a certified payments professional be able to:

- Understand terminal, software and peripheral device setup; ensure the terminal can process transactions;
- Understand the importance of utilizing support from the acquirer and processor to assist the merchant with billing, funding, account maintenance and technical support inquiries;
- Monitor merchant satisfaction to successfully retain merchants and generate new revenue through upsell opportunities and referrals.

**Equipment Set Up**

Each acquirer will have its own suite of technology to offer their customer base. The typical suite of technology is comprised of a physical terminal with all proper connections or software configured to the merchant’s business for the card types that will be accepted. For downloading any terminal, it is recommended by most manufacturers to do so on a Dial-up Analog line.

**Installing on Dial up (Analog)**

Locate the power cord and plug it into the terminal. Have a phone line available and trace it from the wall jack to the back of terminal. It must be able to install on dial up. Plug one end of the phone cable into the terminal base and the other end into phone jack. For dial communication, a prefix may be needed to dial (e.g., 9 or 8 preceding the area code). The prefix can be preprogrammed or initialized at set up.

**Installing on IP (Ethernet)**

Plug one end of the Ethernet cable into the back of the terminal base and the other end into router/switch/hub/internal wiring – whatever is applicable to your location. Due to common communication issues, processing over IP is faster and eliminates most connection issues, except when downloading, which is recommended to take place on an Analog line.

**Installing Peripheral Devices**

A peripheral device may be provided in addition to the credit card terminal. The payments professional will need to determine if peripheral devices are needed and ensure that they are operating properly. Before installing any peripheral device, you must insure that all batches are cleared and the power is turned off to the terminal to avoid blowing encryptions and/or harming the equipment.

Printer – ensures that both the merchant and the customer receive copies of the receipt and that the merchant can print their reports.
PIN Pad – an electronic device used in a debit or smart card-based transaction to input and encrypt the cardholder’s PIN. The PIN pad is required so that the customer’s card can be accessed and the PIN can be securely entered and encrypted before it is sent to the transaction manager of the switch or the bank.

Check Imager – a payment automation device that reads the MICR (Magnetic Ink Character Recognition) information on checks.

Contactless Reader – any pocket-sized card with embedded integrated circuits that can process and store data and communicate with a terminal via radio waves.

**Utilizing Acquirer and Processor Support**

The payments professional should have a working relationship with their acquiring office to understand how their monitoring system works, be aware of alerts, and proactively assist their merchants. Some of the most common issues stem from billing, funding, account maintenance and technical issues.

**Billing and Funding**

Understanding how the customer is billed and funded is essential to identifying when expectations are falling below forecasted performance. The merchant statement is an integral resource to properly price and monitor activity.

**The Statement**

The statement format will vary, but common areas of the merchant statement are:

- **Header Information** – merchant’s business information
- **Deposit Information** – daily account of the month’s transaction information
- **Deposit Item Summary** – a summary of the month’s transactions
- **Settlement/Discount** – the month’s transactions sorted by card type and fees associated
- **Surcharges** – downgraded transactions
  - Description is for the downgrade description
  - Items are the number of transactions that qualified for a particular downgrade
  - Fee amount is the total dollars charged for each downgrade type
- **Other Fees**
- **Total Debited or Credited**

**Account Maintenance**

Account maintenance requests should be closely monitored; they are the first alert of an opportunity to further assist the customer and optimize account performance for increased revenue. Some common account maintenance occurrences are:

- Cancellation requests
- Sales partner complaints (opportunity to improve the one-on-one relationship)
- Request to review and amend rates and fees
- Ownership changes (opportunity for retention, which would require a new merchant application to be signed by the new owner)

**Technical Support**

The payments professional should maintain contact with technical support to ensure the customer is receiving assistance during and after normal business hours. The payments professional may not always be able to be onsite, so an extension of the relationship is optimal to maintain trust and performance.
Monitoring Merchant Satisfaction

Monitoring merchant processing patterns is essential to drive prompt and immediate action to service the needs of your customers and eliminate reason for risk-of-flight.

Utilizing your acquirer and processor notification systems to identify opportunities is one monitoring tool.

Monitoring customer survey results, which are typically conducted quarterly, is another method to provide insight into the merchant’s perception of performance.

Re-pricing, redesigned solutions, and other methods of retention may be necessary to keep the customer processing. As such, value-added services should be utilized as a means of improving merchant satisfaction and retention. Value-adds increase convenience and can increase profit on the merchant account.

Value-Adds

EBT – electronic acceptance of government benefits (e.g., food stamps and/or cash). These cards are generally accepted at grocery stores.

Debit – an ATM bankcard, also known as a check card, that allows a merchant to deduct money directly from a consumer’s bank account. The use of a true debit card requires the cardholder to enter a PIN to complete the transaction.

Gift card/loyalty programs – a magnetic-stripe or smart (chip) card that replaces traditional paper gift certificates. The program is based on gift card usage that generates points in exchange for products and services.

Split Funding – A merchant may receive a capital advance from a third party and direct the processor to repay the third party with a % of their daily credit/debit card processing deposited into the third party’s bank account and the remainder deposited into the merchants bank account.

Checks – a negotiable paper document drawn against deposited funds exchanged with a merchant for payment of products or services.

- Check Guarantee – this is the process of issuing approval codes for check acceptance for merchants. With Check Guarantee, if a check is returned to a merchant for any reason and they followed the proper acceptance procedures, they are automatically credited for the ‘bad’ check and collection efforts are pursued directly with the check writer. While this process is better than regular check verification, the cost is higher.

- Check Verification - this is the process of issuing verification codes for check acceptance for merchants. With Check Verification, if a check is returned to a merchant, they are typically not reimbursed by the processor. Collection efforts will be made on behalf of the merchant at an additional cost, however there is no ‘guarantee’ of payment on uncollected items. Therefore, this service is less expensive than Check Guarantee.

- Check 21 – this is the process of capturing a check at the point of entry (can be point of sale scanner or a picture on a mobile phone). The check image is transmitted to the issuer and paid through the settlement process.

- ACH Debit – this is the process whereby the consumer gives a pre-approval to have funds debited from either their checking or savings account. This is not a real-time transaction and can be subject to non-sufficient funds rejection.

Relationship Building

Maintaining an open and professional relationship with all areas of business is important to keeping the lines of communication open. The payments professional is going to be successful by communicating with customer service, technical support, applications processing and partner support. Maintaining a relationship with risk management and the collections divisions will help the professional stay ahead of notifications, funding holds and other performance concerns.
Task 3: Acquire in-depth knowledge of all participants/components/stakeholders associated with completing a payment transaction in order to be able to explain these same issues to stakeholders.

Objectives

This task requires that a certified payments professional be able to:

- Identify all the participants and stakeholders associated with completing a payment transaction;
- Identify and understand all the components associated with completing a payment transaction; and

Understand and explain the roles of acquirer/member/settlement bank, issuing bank, third-party authorization vendor, merchant/POS device, cardholder, and card brands.

Who are the Participants and Stakeholders?

A **cardholder** is an end user or consumer.

A **card issuer** is any banking institution that provides credit or debit cards to a consumer. Examples of card issuers include Chase, Capital One, Bank of America and credit unions.

An **acquiring bank (or acquirer)** is the bank or financial institution that processes credit and/or debit card payments for a merchant. Examples of acquirers include HSBC and Wells Fargo.

A **payments processor** is a company (often a third party) appointed by a merchant to handle payment card transactions for acquiring banks. There are two types of processors: front-end and back-end. Front-end processors have connections to various card issuers and supply authorization and capture services to the acquiring banks’ merchants. Back-end processors accept settlements from front-end processors and, via The Federal Reserve Bank, move the money from the issuing bank to the merchant bank. Examples of payments processors include Global Payments, First Data, Chase Paymentech, TSYS, and Elavon.

A **merchant** is any business that accepts credit or debit cards for payment in exchange for goods or services. Examples include Amazon, Target and Best Buy.

A **card brand** is a network of issuing banks and acquiring banks that processes brand-specific payments. The best known card brands are Visa, MasterCard, American Express, Discover, JCB and China UnionPay.

An **Independent Sales Organization (ISO)** is an organization or individual registered with a card brand (Visa or MasterCard), and has a payment card relationship with an acquirer or issuer to perform functions on behalf of the acquirer or issuer (i.e., the ISO soliciting merchant accounts, arranging for terminal purchases or leases, providing customer service, and soliciting cardholders). Examples of ISOs include Total Merchant Services and North American Bankcard.

A **service provider**, more commonly known as a merchant service provider (MSP), is a company or organization that provides transaction processing solutions to merchants; any sales office that offers payment services to merchants.

Components

There are two main types of payment cards – debit and credit.

A **debit card** (also known as a bank card or check card) provides the cardholder electronic access to his or her bank account(s) at a financial institution. Examples include Visa or MasterCard check cards or Debit Network cards that are used with a PIN in an ATM,
such as NYCE, STAR, and PULSE. These cards are issued by a bank and attached to an individual’s checking account. A debit card may be used used used authorized by one of two different methods:

- Pin-based – The cardholder enters a 4-digit pin number and the transaction, is routed through a debit network real time posted
- Signature – The transaction is routed through the credit networks

A credit card allows the cardholder to buy goods and services based on the cardholder’s promise to pay for these goods and services at a later date. The card issuer creates a revolving account and grants a line of credit to the cardholder from which the user can borrow money to pay a merchant or use as a cash advance. Examples include Visa or MasterCard credit cards issued by a bank and attached to a line of credit.

A Point of Sale (POS) terminal is a device that processes transactions with a debit or a credit card, via a telephone line or Internet connection, typically powered by a power cord.

A wireless terminal is a device that processes transactions with a debit or a credit card via a cellular (wireless) data network, typically powered by a battery pack.

A mobile payment solution consists of a device and software application (typically a smart phone application and card reader) that process transactions with a debit or a credit card via a cellular (wireless) data network. Examples include Payment Jack and Square.

A virtual terminal is a payment gateway service provider allowing merchants to accept credit card and electronic check payments through their website over an IP (Internet Protocol) connection.

PIN Pads / PIN Entry Devices (PEDs) are electronic devices used in debit or smart card-based transactions to input and encrypt the cardholder’s Personal Identification Number (PIN).

Transactions

Authorization – The cardholder presents the card as payment to the merchant; merchant submits the transaction to the acquirer (acquiring bank) through the payment processor. The acquirer verifies the credit card number, the transaction type and the amount with the issuer (card-issuing bank) and reserves that amount of the cardholder’s credit limit for the merchant by use of an authorization code. An authorization will generate an approval code, which follows the life of the transaction through the processing systems.

Batching – Authorized transactions are stored in batches, either in the terminal or on the processor’s host, which are sent to the acquiring clearing processor on a predetermined schedule, also known as “auto batch”. If a transaction is not submitted in the batch, the authorization will stay valid for a period of time, determined by the issuer, after which the held amount will be returned to the cardholder’s available credit (see authorization hold). Some transactions may be submitted in the batch without prior authorizations; these are typically seen where the authorization was unsuccessful but the merchant still attempts to force the transaction through. (Such may be the case when the cardholder is not present but owes the merchant additional money, such as a hotel stay extension or car rental.)

Clearing and Settlement – The acquirer sends the batch transactions through the card brand, which debits/credits (if chargebacks and returns exceed sales for the day) the issuer for payment and credits/debits the acquirer. Essentially, the issuer pays the acquirer for the transaction.

Funding – Once the acquirer has been paid, the acquirer pays the merchant. The merchant receives the amount totaling the funds in the batch in total or less the discount fees charged.

Chargeback – A chargeback is an event in which money in a merchant account is held due to a dispute relating to the transaction. Chargebacks are initiated by the cardholder or the issuing bank. In the event of a chargeback, the issuer returns the transaction to the acquirer for resolution. The acquirer then forwards the chargeback to the merchant, who must either accept the chargeback or contest it.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 4

DOMAIN 4: PRODUCTS/SOLUTIONS/MOBILE TECHNOLOGY

Task 1: Ask merchant-specific qualifying questions in order to evaluate and ultimately meet or exceed merchant-specific needs.

Objectives

This task requires that a certified payments professional be able to:

- Listen to, hear, and understand merchant needs in order to recommend solutions based on voiced concerns, issues, and goals.

Qualifying Your Merchant

Determining the appropriate products or services for your merchant will differ somewhat based upon whether your merchant is new to accepting credit cards or already accepts credit cards. In either case, the goal is to ensure that you are properly addressing the payment processing needs and ancillary services required to appropriately service your merchant. The qualifying questions can be broken out into three distinct categories. What payment types or ancillary services need to be supported and/or are desired? What is the payment processing environment? What is the impact of change or addition of services on staff and support teams?

Payment Types

Identifying the payment types required by the merchant starts with the card brands and then moves into other payment mechanisms, including check, ACH or gift. Further, there may be requirements for additional data exchange as part of the payments process or apart from the payments process. The following is a partial list of items to discuss when identifying the payment types and ancillary solutions required by your merchant.

- Determine need or desire to accept primary payment brands, including Visa, MasterCard, Discover, American Express or JCB.
- Need for purchasing card support, including level 2 or level 3 data.
- PIN debit, with or without cash back and which networks, including routing order do they desire to support.
- Check verification, guarantee, Check 21, or other Check Processing Products.
- ACH debit services.
- Gift card processing, including support for an existing gift card program.
- Loyalty or reward programs in conjunction with the payment method.
- Private label / proprietary cards
- Dynamic currency conversion or multi-currency processing to support foreign cardholder transactions.
- Need for chip card processing or foreign card types such as China UnionPay to support foreign cardholders.
- Merchant Funding options to give the merchant access to capital
- Mobile Wallet/NFC services, such as ApplePay, SamsungPay and GooglePay
- Reporting and Integration needs such as QuickBooks accounting systems
- Specialized reporting by vertical, such as Tip reporting, Reservation management, etc
- Equipment needs – i.e. POS Terminal, Virtual Terminal, gateway, etc.

Payment Processing Environment

Understanding the payments processing environment is just as critical as understanding the variety of payment types. Selling a solution designed specifically for a merchant is the preferred method. Additionally, the differences between restaurants,
hotels, e-commerce, MOTO or petroleum merchants are significant, and each requires individual solutions to meet their specific needs. With this in mind, the following should help in guiding the appropriate solution set and are valid regardless of industry.

- Number of transactions processed along with peak transaction volume.
- How is the sale completed today?
  - At the counter, at the table, in the field, over the phone, on the internet or all of the above?
  - Customer facing or processed by the business?
- the merchant use a third party for taking the order or for placing outbound calls?
- How fast do the transactions need to be processed?
  - What is the throughput requirement?
  - Is it batch processing at the end of the day?
    - Does the merchant prefer to manually reconcile and submit their batches of Transactions (Manual) or are they willing to let the POS system generate the end-of-day batching (Auto Batch)?
    - Monthly billing vs. Daily billing
- What type of IT staff is available for the merchant?
- Is high-speed Internet available or only dial-up?
- What inefficiencies exist in the current processes?
- What type of fraud protection tools might be required?
  - AVS, CVV, IP validation, velocity checking, PIN, etc.?
- What type of hardware and software is in place today?
  - Is it PCI compliant, and what is the functionality?
- What functionality is desired in their hardware or software, and why do they desire this functionality?
  - Do they want an integrated solution or a standalone solution, and why?
- Is there a budget allocated for hardware or for software changes?
  - Do they even know if there is a cost with software changes?

Asking these questions, and many others, will help determine the appropriate product solution for your merchant. These questions are a small representation of the questions to ask and are designed to drive further questions.

**Merchant Impact**

All of the previous questions designed to understand the merchant environment are also relevant to the impact a potential solution has on the merchant processing environment. The next step in the process is to ensure understanding of the solutions’ impact upon the merchant. Using the same questions, we now drive to the impact the answers may have on your recommended solution.

- What is the number of transactions processed along with peak transaction volume?
  - This question is asked to help understand the technical throughput required for the merchant’s processing volume. If you suggest a dial terminal and they process a hundred transactions a day, your merchant may not have enough throughput-throughputs. Is a high-speed option a better choice? If thousands of transactions per day will be processed, do they need a more dedicated solution to the processor?
How is the sale completed today?
- Defining how the sale is completed helps determine the hardware or software solution(s) required. If it is a restaurant with a seasonal patio that needs payment processing at the table, then it might be appropriate to have a device inside the restaurant and another portable one for the patio. If it is an e-commerce environment, do they need batch processing or is real-time a requirement? Can you improve the plumber’s efficiency by providing a smart phone solution as opposed to them calling the office? If the order is processed by a third-party, what type of controls does the merchant need, or is the merchant fine completely outsourcing?

How fast do the transactions need to be processed?
- The merchant may accept a minimal number of credit cards, but if the processing ties up resources, they may want a high-speed solution. Consider the impact of batch processing at night for MOTO merchants. Do they need real-time authorizations, or is an internet-based secure processing solution that can store and process in a batch environment sufficient? Do they have a need to store cards for recurring billing, and what mechanism do they have in place to work with a suggested third party.

What type of IT staff is available for the merchant?
- You may be able to provide a comprehensive processing solution that ties inventory, accounting, payments processing and customer services into a seamless package. However, if the merchant does not have the ability to integrate their components or the staff to manage the solution, perhaps a more streamlined solution is in order. On the other hand, if the merchant has an in-house IT staff it is important to understand their capabilities and willingness to support outside solutions. Take the time to communicate up front to ensure your solution works for their environment.

What inefficiencies exist in the current processes?
- This question gives you the opportunity to provide a solution that not only fits their payments needs, but addresses inefficiencies of the existing processes.

What type of fraud protection tools might be required?
- This question, designed to ensure you have the appropriate solution, also provides you with an opportunity to educate the merchant and to understand what pain points they have so that you may build a solution to fit what they know and what they don’t know.

What type of hardware and software is in place today? Is it PCI compliant, and what is the functionality?
- If the merchant has a stand-alone terminal, this question helps determine whether you can re-program the device, how many devices and whether their software is compatible with your software. Understanding who supports the software or device is as critical as to whether you can re-program the device.

Is there a budget allocated for hardware or for software changes?
- At the end of the day, you need to understand the merchant’s cost constraints to ensure your proposed solution is in line with their processing needs as well as their financial goals.
Task 2: Determine the optimal solution from all available product configurations to satisfy or surpass the merchant’s needs.

Objectives

This task requires that a certified payments professional be able to:

- Explain the features, benefits, and differences across solution offerings and how specific solutions can meet specific merchant goals.

Product Solutions

After completing Task 1, you should be in a position to recommend the appropriate solution(s) to your merchant. Implementing the best solution may require partnering with third-party software or hardware providers or providing technical support to the merchant’s in-house development team. Regardless of the solution offered, you are responsible for the payments processing capabilities of the system and must ensure you or your chosen partners are capable of supporting the solution. Thus, for Task 2, it is necessary to understand a wide variety of solutions from implementation through support. Understanding specific functionality is as critical as understanding the broader goals of a recommended solution. The remainder of this section is designed to provide you with thoughts and ideas on solutions available and is by no means meant to be a complete listing.

Processing Hardware

Payment processing hardware comes in many different shapes and forms. While not a complete listing of the types of hardware in use in the marketplace, familiarity with the following hardware solutions is required.

- Traditional terminals such as countertop, wireless, mobile, and Point-of-Sale are the most prevalent for processing for the small to midsized merchant. A variety of terminal applications are available for these devices including those specific for restaurant, hotel, retail, check card, Check21, and gift/loyalty. Many others that a merchant may desire are available from processors, third parties or System Integrators (Value Added Resellers (VARs)).

The functionality of these terminals varies greatly. The following is a sampling of the functional elements of these devices:

- Dial or Dual Comm (Ethernet connectivity)
- Multi application or single application
- Stand alone printers or integrated printers
- Custom receipts or standard receipts
- Integrated chip card processing
- Stand alone PIN pad or integrated PIN pad
- WiFi or wireless modems
- Battery operated
- Touch screen displays
- Check reader connectivity
- Network connectivity amongst devices
- Contactless or Near Field Communication (NFC) support
- EMV Reader Stand alone or integrated.
- Mobile reader operating in the Mobile phone audio jack
POINT-OF-SALE (POS) systems provide merchants with functionality that is more sophisticated than that available in the traditional terminal. Most POS systems are primarily developed and used for specific, such as the hospitality industry or for the restaurant industry. When recommending or preparing to support an existing POS solution for your merchant, the following should be considered:

- Connectivity method to the processor (dial, SSL, dedicated)
- Processors supported by the POS system software
- Installed and serviced by a VAR or directly
- Third party applications supported including check, gift, loyalty, chip or PIN debit
- Who will be supporting the installation of the system
  - Will there be costs and is the merchant willing to pay to make changes to their merchant services
- Benefits of a proprietary system offered by a processor or a generally available solution in the market

- PCI Compliance
- Hardware and/or Software upgrades that may be available and/or required prior to making changes to the merchant services, as well as the cost of these upgrades
- Ancillary services required by the merchant
  - Inventory management
  - Time and attendance
  - Remote receipt printing
  - Network capabilities for remote reporting
- Third party gateway providers in the middle of the transaction
  - PCI compliance
  - Benefits provided by the gateway
- Petroleum solutions
  - Pay at the pump
  - Inside counter sales
  - Fleet card types accepted
  - Software integrated on a controller to support multiple devices

SOFTWARE, E-COMMERCE AND CARD-NOT-PRESENT (CNP) solutions range from those completely managed and supported by third-party providers to software installed and supported by the merchant. Task 2 requires an understanding of the following:

- E-commerce gateway providers
  - Batch processing, fraud tools, one time or recurring payments, fulfillment center integration, order validation, delivery methods
  - Hosted payment page, integration options, card data storage
  - Online malls
  - Multi-currency processing

- Retail or card present gateway solutions
  - Software as a Service (SAAS)

- CNP service providers
  - Batch processing, real-time, recurring payments, account updater, fraud tools, fulfillment center integration, order validation, ACH, check, etc.

- General technologies such as tokenization, encryption methodologies, end to end encryption (E2E or P2P), peripheral devices, remote access tools, browser support, report delivery (SFTP, FTP) and integration methods.
Merchant Support

Ensuring your merchant has appropriate full-service support for the products and services you have recommended and/or installed, is critical to the long-term success of your business relationship. Support is often divided amongst the processor, the software provider and the merchant acquirer. Below is a listing of support requirements or industry terms to consider when recommending or agreeing to support a merchant’s processing solution.

- Know which terminals your processor has certified as Class A or Class B
- Stage-only
- Information required to program the software
  - VAR program information sheet
  - Terminal download information
- SoftPay, TermMaster and other application download programs
- Terminal deployment, repair and supplies
- PIN pad encryption and key injection
- Peripheral support
  - Smartphone sleds and dongles
  - Wedges or mag stripe readers for POS systems
  - Check readers
- Gateway escalation process between your merchant and the processor
- Quick reference guides, online support forums and other technical resources available for use within your organization and by the merchant
- Billing for third party services and the ability to audit or escalate discrepancies
- Making changes to the application in the terminal or software
  - Who, how, when, and at what cost?
- Number of years in business and financial strength of the business partners
- Average speed of answer at the support desk
- Knowledge level of help desk along with an escalation path for you and for your merchant
- Defined service levels and metrics used to track service levels

As stated previously, the items identified in Task 2 may not be complete, or applicable for each and every situation. These items have been identified as the areas typically addressed during the process, with which you should be well versed when working with a variety of merchants. It is suggested that you work with your processor and third-party service providers to further understand the nuances between supporting and selling a straightforward dial terminal vs. an integrated POS system. Further, with the proliferation of smartphones, contactless payments and emergence of chip card processing in the United States, it is ever more important to keep abreast of new technologies and the potential for a positive or negative impact - to your merchant.
Task 3: Fully test and train the merchant on all new solutions, whether installed by a third party or employer, in order to ensure a fully prepared, educated, and active merchant.

Objectives

This task requires that a certified payments professional be able to:

- Understand technically sophisticated solutions and their operation; and
- Effectively communicate to and with audiences of varied technical savvy.

Training and Testing

The depth of knowledge required for training your merchant on processing their payments depends upon the equipment installed, the role of third parties, and the knowledge level of your merchant. Merchants with existing equipment that is being reprogrammed may require little or no training. However, merchants receiving new terminals or POS systems will require more in-depth training. Task 2 focused on the types of solutions available to merchants and touched briefly on the support and some of the technical components required for successful processing. With so many solutions available, rather than an in-depth analysis of each service offering, the content for Task 3 will focus on the types of training your merchant should receive.

General Training Requirements

Training your merchant begins with a thorough understanding of the card brand rules and how they affect the merchant’s POS environment or processing systems. Further, if you have sold, or are supporting methods of payment that include check verification, guarantee, Check21, ACH processing or gift card programs, you should perform the same sort of training for those programs as you would a traditional card acceptance program. Performing a test transaction for each product and reviewing the quick reference guides is always helpful in training the merchant. The training session is also a good time to also discuss PCI Compliance procedures to help your merchant better understand these strict requirements. Training for card payment processing should cover the following points:

- Transacting a sale
- Demonstrating the use of an EMV reader which will hold the card through the transaction versus a swipe of a card.
- Issuing of refunds or voids: the how, when and why for each transaction, along with where this occurs in their software or processing device.
- Receipt truncation and how to acquire the full card number should they need to issue a credit or an adjustment.
- An overview of the timeframes and rules for chargeback processing, ensuring that they understand the importance of a timely response and that they know where to look for the information in their systems to respond to a chargeback.
- Duplicate batches are not a common problem with processing; however, your merchant should understand the potential for fines and what to do if they suspect that a batch has been duplicated.
- Storage of card data:
  - When it is allowed?
  - How it is to be stored?
  - What capabilities exist for secure storage and access with their processing systems?
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 4

- A thorough understanding of the fraud tools available to your merchant, whether processing CNP or card present, is a critical training component.
  - Key entered AVS, signature matching, card identification characteristics
  - AVS, CVV responses, approvals, IP validation checking, expired cards and other tools for CNP merchant
  - EMV as a fraud prevention tool?
  - A discussion that an approval is not a guarantee of a good transaction.
  - Ensure they understand the timeliness for settlement and rules regarding authorizations.
  - Issuing of credits to an offsetting transaction
  - Other tools that may exist within or for a particular solution

- Card acceptance rules for credit, debit, prepaid and other schemes to ensure that the merchant does not run afoul of card brand rules.
  - An example is the reciprocity agreement between Discover and JCB, Union Pay, BC Card, etc.  These international card brands work at Discover accepting merchants.

- Discuss the telephone numbers available for support and which numbers to call for different types of issues.

- Balancing the batch settlement reports vs. the merchant statement.
  - Your merchant should understand what reports are available in their systems and how they relate to the month end merchant statement.

**Technical Training Requirements**

The technical training involves the use and operation of the device or software along with the processes to handle the “what-if” scenarios that occur during the payment acceptance process. As a straightforward process, technical training can be broken down into three distinct segments:

- installation or integration of the device or software
- use of the device or software
- the communication technology of the device or software.

Installation and integration will depend on the processing solution implemented. We have broken out highlights for CNP/e-commerce and software, traditional terminals, and wireless devices.

Traditional terminal technical training should cover the following elements:

- Power and connectivity of the device to the payment processing network. This may include connectivity to a physical or wireless internet network, power and/ or telephone line.
- Attachment and or use of peripherals including printers, PIN pads, CHIP card readers, contactless card readers, check readers or other devices attached to the terminal.
- The various error messages produced by the device along with where and how to fix the errors. This could include rejected batches, communication errors, dial tone errors, duplicate batches or changes to receipt verbiage.
- Use of the terminal including processing sales, credits, voids, settling batches, reversal transactions, partial approval transactions, PIN debit, balance inquiries, clerk or server reports and other functionality of the application residing in the terminal.
- Downloading or accessing additional applications or services connected to the device.
- Troubleshooting tools available in the terminal.
E-commerce, CNP and software solutions have many of the same technical training components as a traditional terminal. However, the depth of the technical solution typically extends beyond the merchant’s systems and will include the following elements in addition to those required for the traditional terminal. These may not be applicable to every situation and may be a subset depending on the complexity of the systems.

- Installation of payment processing software
  - Operating system version compatibility with software, hardware and firmware
  - Browser support required
  - User control and access
- Configuration of routers, firewalls and access to the systems
- Administration, setup and configuration of account on the gateway or e-commerce software platforms. Building the TID information into the systems.
  - APIs required for authorization, settlement and reporting
  - APIs required for hosted payment pages
  - Upload of initial data for recurring payments
  - SSL certificates for secure web processing
  - Integration tools with accounting or back office software
  - User hierarchy
- Configuration of peripherals and validation of functionality
- Troubleshooting and reporting tools available to assist merchant with support calls, including communications issues and third party integration concerns.
- Network connectivity for the various stations and consolidated reporting at the processor level should be validated.

Wireless devices provide a few nuances that build upon the terminal and software environments. Most notably, wireless devices have reporting tools for network access, WiFi to mobile network communications options, and a variety of hardware and application options. Helping your merchant move from a stand-alone environment to one on the move is achievable, but take the time to ensure your merchant has adequate familiarity with the device and application to function in the field. Special attention should be paid to the application in use, the swipe devices and the diagnostic tools available, including those from the application and hardware providers, not just the processor.
Task 4: Demonstrate a complete understanding of challenges, issues, requirements, and/or opportunities, and have the knowledge to properly troubleshoot each maintenance situation.

Objectives

This task requires that a certified payments professional be able to:

- Identify the resources available and guide the merchant to those resources for the various maintenance issues which may arise; and
- Navigate the technical environment of payments processing in a manner that is efficient and timely for the merchant.

Support Resources

Properly supporting your merchant’s payments processing needs is important for merchant retention and often involves multiple resources. Your ability to understand the basic requirements AND the resources required for support is critical in managing expectations and the ongoing merchant relationship. As an example, a merchant with a dial-up terminal requires a fundamentally different support infrastructure than a merchant to whom you have sold an integrated POS system or one operating an e-commerce website. With this in mind, what are the variances and resources available to you, and with what should you be familiar?

- Class A vs. Class B support from the payment processor.
  - Understand what these terms mean, HOW your merchant can reach the processor, and WHEN they should reach out to the processor.
  - Methods for reaching the support, including e-mail, web chat, telephone, discussion forums and online portals.
- An understanding of Level 1 vs. Level 2 operational support from a service provider.
- QRGs terminal templates and user guides available for your merchant.
- Where or who does your merchant call for terminal supplies, receipts, or if a terminal or PIN pad needs to be replaced?
- Back office support for answering questions regarding chargebacks, statement questions, ACH, balancing or batch issues often is different than the support for the terminal or payment application.
- What are the requirements to support a third party VAR application (e-commerce or web based) and how does this differ from supporting a standard POS terminal?
  - Programming the application
  - Managing discrepancies between the POS data and what was processed at the settlement level
  - Who manages the installation and updates for the initial deployment, and who is responsible for ongoing card brand enhancement, maintenance and support?
  - Researching authorization issues
  - Troubleshooting communications issues between the POS, within the store, and with the website
  - Integrating a payment application with the shopping cart or VAR
  - Use of third party payment software as part of a POS application, who provisions this software, and what are the pitfalls of using a third party application?
  - Who is responsible for PCI, and what is the process for obtaining PCI compliance with each of the parties involved in the POS or web environment?
- How the use of third-party applications such as check processing, gift card or loyalty can be integrated at the POS
  - Separate applications or combined applications?
  - Single support source for help or multiple endpoints for support?
  - What is the billing process, and what are the merchant’s expectations?
The process of supporting a merchant is no longer as simple as telling the merchant to call a single 1-800 number for support. The complexities of software systems, web environments and the various applications used by merchants mandate an understanding of the multiple touch points affecting the merchant and the responsibility of each touch point in supporting the merchant. The bullet points above are illustrative of many elements of support, but are not intended to be all inclusive.

Task 5: Demonstrate a broad understanding of technologies and products within the payments processing industry to meet current and future regulatory requirements.

Objectives

This task requires that a certified payments professional be able to:

- Understand and communicate the high level technical needs of processing at the merchant level; and
- Understand and communicate how processing works today in relation to new technologies, as well as the impact of technologies and regulations on the processing environment as it exists today.

Technologies and Products

The previous tasks covered in Domain 4 outline the various products, services and technologies involved in payments processing. Understanding when, where and how these technologies are used today is essential to understanding future changes in technology and regulation. Utilizing these sections as a baseline for Task 5, we can segregate technologies and products into the following categories:

- Card technologies
- Processing hardware
- Processing software
- Communications technologies
- Value added programs

The magnetic stripe has been in existence since the early 1960’s. Since that time, the basic technology has not really changed. Smart cards, first used in pay phones in France in 1983, were eventually ported to payment cards in 1993, as Visa, Mastercard and Europay created the EMV standard for card processing. Smart cards represent the single biggest change merchants and processors face in transaction processing, as they can be used on the physical card, over the internet, in mobile phones enabled with NFC, in ancillary devices such as key fobs, and integrated with loyalty, rewards and banking functionality, all local on the chip itself. It is important to understand how chip cards are used throughout the world so that you may have an understanding of future impact to your region. Key points include:

- Online vs. offline chip
- Signature vs. PIN
- NFC
- Chip application segmentation capabilities
- Payment chip for mobile vs. mobile wallets
- Hardware required for processing chip cards
- Brand regulatory requirements
Processing hardware previously meant the knuckle-buster and perhaps a telephone for obtaining an authorization number. Today, the payment hardware used is an integral component of the consumer and merchant experience. Beyond the traditional swipe devices built for the purpose of POS terminals and integrated systems, it is also necessary to understand the technology and meaning of the following components, not only to your business, but to merchants as well.

- End-to-End or Point-to-Point encryption
- Integrated chip card processing vs. peripheral device options
- Encrypted hardware deployment requirements
- Biometric payment options – as they arise
- Contactless or NFC readers
- Dial to IP solutions
- The proliferation of kiosks and other unattended payment options

Processing software can mean something as simple as a PC-based application loaded to a computer by CD to an enterprise-wide system integrated with supply chain management, marketing and financial systems. With technological advances, these systems continue to evolve, provide new business opportunities, and create operating efficiencies for your merchant. These same technologies can often be nothing more than "noise" that must be carefully evaluated prior to engaging your merchant for recommended processing solutions. Further, your ability to remain current and up-to-date on new software solutions can help with merchant retention while providing new revenue opportunities. Some of the software terms and solutions you should be familiar with include:

- SAAS and Cloud Based computing
- Virtual terminals
- Electronic Bill Payment and Presentment (EBPP)
- Software for specific operating systems, including iOS, Android, Windows, MAC, Oracle
- Real-time vs. batch
- XML, JAVA, use of APIs and other methods of software integration
- Tokenization and other card storage solutions
- Shopping carts, web hosting, web site development tools and integration needs
- Systems reliant upon the payment processing data for internal uses, including accounting, inventory management, billing and other systems

Communications technologies can mean everything from a dial-up phone line to satellite based systems used to deliver card (and other data) to host and processing systems. You should discuss the benefits of various communication technologies with, and provide recommendations to your merchants. Some of these include:

- NFC and contactless communications
- WiFi vs. cellular based processing solutions
- Smart phone vs. traditional wireless terminal
- Access to the network during peak periods
- Dedicated circuit technologies
- Often called leased line, frame or IP circuits
- Dial solutions
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 4

- SSL vs. the physical connections, including SSL, cable internet, DSL or satellite
- When and how a transaction is determined to be billed at an IP rate by the processor vs. a dial or SSL rate
- Path of transaction from merchant’s systems to the processor, including possible points of failure such as the telephone company or the hosting provider
- Potential for use fees or regulatory changes affecting the use of communication technologies

Value added programs are programs that provide your merchant with operating efficiencies as well as programs that surround the consumer experience with the merchant. While many of these are not part of the actual card processing solution, the importance of the impact of these types of solutions cannot be underestimated. When considering the following, do so with an understanding of the consumer experience, the merchant benefits, integration requirements, and back office support and associated reporting for each mechanism:

- Gift card processing
- Check guarantee and verification
- Prepaid functionality, including balance inquiry, partial approval, etc.
- Loyalty
  - Punch card functionality
  - Discount off purchases
  - Card-based rewards program
  - Redemption of rewards
    - Mobile
    - Paper
    - Physical card
  - Offer-based programs
- Marketing programs
  - Google, Facebook, Groupon, Living Social, and others
  - Move to instant rewards
  - Text-based and e-mail marketing
- Use of mobile devices and contactless fobs to affect payment and initiate rewards functionality with the merchant
- Understanding of the privacy laws and regulatory requirements surrounding existing programs and new programs as they come to market

Payments processing, or more importantly, moving money, is a heavily regulated business. Critical to long term success is understanding current regulations, keeping an eye on future changes, and understanding how these changes may affect your business model and your merchants’ practices. The regulatory and compliance domain provides an overview of current regulations as well as helpful resources to monitor new regulations.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 5

DOMAIN 5: RISK

Task 1: Evaluate specific merchant characteristics regarding how the merchant conducts business to determine merchant fit with corporate and industry specific objectives

Objectives

This task requires that a certified professional be able to:

- Understand general industry requirements as well as sales organization credit policies to determine if a potential merchant is a fit within the selected sales organization;
- Identify and understand merchant classification via Merchant Category Code (MCC) guidelines; and
- Explain the difference between a Prohibited card brand merchant and a High Risk potentially allowed merchant.

Is a merchant a fit for the selected sales organization?

Depending on the size and sophistication of the organization you represent, you will be able to pursue, and service a variety of merchants. Typically credit policy is set at the acquiring bank level and passed downstream to the sales organization for implementation. In many cases the size and sophistication of the sales channel will enable a wider spectrum of merchants to be boarded, for example: bleeding edge technology channels, or enhanced due diligence merchants.

Some sales organizations may have stricter guidelines due to the contractual relationship that is in place, or due to their specific risk appetite.

Generally you will follow guidelines that clearly outline permitted, restricted, and prohibited merchant types. You are typically able to support merchants under the permitted category with less stringent underwriting, and minimal restrictions. Restricted merchants can be on-boarded with enhanced due diligence controls (examples are: volume restrictions, reserves, additional financial guarantees) in place. Prohibited merchant types are prohibited by the acquirer and may not be solicited.

MCC Guidelines

A Merchant Category Code (MCC) is a four-digit code that identifies a merchant by their business line. It is similar to a Standard Industrial Classification (SIC) code, but it is specific to the acquiring industry. The MCC is assigned by the acquiring bank or sales organization when a merchant initially begins accepting credit cards. The MCC is assigned to the merchant based on its primary business (i.e. Goods or services sold). For the purpose of this exam we will focus on MCC codes as they are used most often in the merchant acquiring space.

Merchant Category Codes can be looked at in two different ways:

- By grouping of similar MCCs that fit a particular business category, or
- By individual MCC that describes the business type in detail.

Prohibited/High Risk Merchant Categories

The card brands have very strict guidelines around the types of merchants that can be supported. They have designated some merchants to be either Prohibited meaning that transactions are not allowed under any circumstances, or High Risk, meaning that under certain conditions (i.e., risk structure in place) these merchant types and transactions may be allowed. The restrictions are not uniform between sales organizations. For the purpose of this section we will use guidelines from MasterCard and Visa.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 5

Visa has developed a program requiring merchant acquirers that support high risk merchants to register any merchant with the following MCC code:

- 5967, Direct Marketing – Inbound Teleservices Merchant (adult content)
- 5966, Direct Marketing – Outbound Telemarketing Merchant
- 5962, Direct Marketing – Travel-Related Arrangement Services
- 7995, Betting, including Lottery Tickets, Casino Gaming, Off-Track Betting, and Race Tracks
- 5122, Drugs, Drug Proprietaries, and Druggist Sundries
- 5912, Drug Stores and Pharmacies

This is a representative list (the actual lists are more detailed) from Visa and MasterCard outlining merchants considered to be prohibited. Acquirers that process transactions for these types of merchants are subject to fees and/or fines.

- Illegal prescription drugs
- Illegal tobacco sales
- Deceptive marketing practices
- Counterfeit and copyright infringing merchandise
- Child pornography
- Illicit websites depicting violence and extreme sexual violence
- Bestiality

Task 2: Compare merchant’s actual results against application assumptions to retain merchant and/or prevent losses.

Objectives

This task requires that a certified professional be able to:

- Identify the variances between legitimate transaction processing and potential fraud processing;
- Understand the risk impact associated with face-to-face transactions vs. card-not-present transactions; and
- Analyze transactional data vs. application data to prevent fraud or loss, while maintaining a knowledge of merchant vs. industry standards for a particular merchant type.

Merchant Characteristics

Over the course of time your organization will encounter cardholder fraud. Fortunately, with due diligence up front and vigilance in the monitoring of your merchant’s transaction processing data, it is possible to mitigate your risk for potential loss. The neural network? and other technologies in use by the card networks and risk management systems available from the merchant processors and other vendors make the task easier now than in the past. It is the use of human capital, ongoing diligence, and interpretation of data provided by these tools that together, provide effective risk management.

Preventing merchant initiated fraud starts with underwriting and evaluating the merchant application. Underwriting is more than simply checking the credit history of the owner and long term viability of the business. You are underwriting the product and/or service sold as well as the merchant’s current and future ability to sell goods and services and to subsequently support the products sold. Sales volumes, transaction volumes, method of processing, previous processing history, inventory, credit history, payables history, debt, income and expected transaction processing volumes all should be evaluated and captured for future use by the risk management team or processing systems.
Valid Processing or Fraudulent Processing?

Key items to monitor include:

- **Maximum ticket** – risk systems must monitor the average ticket and a maximum ticket. Transactions above the maximum ticket may be an indicator of misinformation during the application process, a change in the merchant product, cardholder fraud, a bust-out scheme, or perhaps collusion and should be reviewed and possible investigated.

- **Average ticket of the merchant** – if the application shows a $30 average ticket and you see an average ticket of $400, you should investigate to ensure they are selling what the application stated. Alternately, it could be a fraudulent cardholder transaction.

- **Monthly volume** – applications typically request the average monthly volume and a peak season volume. Sales beyond these volumes may indicate risk problems or may warrant adjustments in account set up to off set merchant growth. Larger than expected volumes in the first month may be an indicator that the merchant has past sales they are trying to process, a bust-out scheme, or that the application was erroneous or false. The volume should also be balanced against similar merchants. Larger volumes than similar merchants may be an indicator of risk and should be investigated.

- **Large dollar or excessive credits** – monitoring credits is a good way to gauge the satisfaction of your merchant's customer with the products and/or services sold. Excessive credits may indicate money problems at your merchant. Large dollar credits may be an indicator of a merchant utilizing the card schemes to layer money amongst their various accounts. It is required that all credits have an offsetting sale. Credits without an offsetting sale may be an indicator of employee theft, merchant system hack, or a fraudulent merchant. Frequent credits for large amounts may be an indicator of money laundering.

- **Duplicate transactions for same cardholder**

- **Chargeback monitoring** – if your merchant is receiving a lot of chargebacks, you should quickly evaluate the reason codes behind the chargebacks and question the merchant's practices. Increased chargebacks may mean your merchant's business is in financial distress, is experiencing supplier issues, or has gone rogue and is committing fraud, potentially against the consumer. This is especially the case if the chargebacks are for unauthorized charges, services not received, or duplicate transactions.

- **Percentage keyed vs. swiped** – monitoring the percentage of swiped transactions vs. keyed transactions is a simple way to tell whether your merchant has shifted from retail to MOTO (mail or telephone order) or internet. If you see more keyed transactions than indicated and subsequently approved on the application, you should talk with your merchant to understand why transactions are being keyed. Increased key-entered transactions may also be an indicator of factoring or money laundering where the cards are not present.

- **Repeat or excessive authorizations** – evaluate authorization logs to help determine whether your merchant has software problems that cause repeated authorizations or whether your merchant is being targeted by a fraudster seeking to find good card numbers. Monitoring excessive authorizations is also a way to help your merchant avoid brand fees associated with non-settled transactions.

- **Merchant information changes** – another area to monitor is when merchants change checking accounts, contact information, or websites. It is important to understand why the changes are being made, how often, who is authorizing the changes, and what impact the changes might have on the business.

The data points listed above are representative of those that a risk department will review. Generally, risk systems have many more parameters and can review a multitude of other transaction values. Remember there are always perfectly valid reasons for variances in any of the data points being monitored. You can contact the card issuer for help in investigating a transaction directly with the cardholder. If you are still uncomfortable, you can work with the acquirer and merchant to implement reserves, delay funding or limit the transaction amounts and volumes until such time as you are comfortable with the business.
Face-to-Face vs. Card Not Present (CNP) Transactions

As a general rule, face-to-face (retail) or card present transactions are less risky to acquire than card not present or CNP transactions. This does not mean, however, that card present transactions are free of risk. For the sake of this study guide, we will consider face-to-face transactions as those where the cardholder is present, the card is able to be swiped or chip read (EMV cards), and authorizations take place in real time. CNP transactions are any transaction where the card cannot be physically processed. These may be where the mag stripe cannot be read, the chip cannot be read, mail or telephone order (MOTO), e-commerce or recurring transactions (where the first sale was not card present). The remainder of this section provides an overview of the key risk factors associated with each processing method, ways to identify the risks, and suggested areas of research.

Face-to-Face Transactions

A misconception exists that there is no measurable risk to an acquirer when signing retail merchants. While the risk is reduced, there are instances when retail processing presents risk that the acquirer needs to anticipate and monitor.

- **Financial strength of the business** – Periodically checking the financial health of your merchant and watching trends in processing volume can help protect against unexpected financial loss. If the merchant is struggling to cover their costs of goods it is possible owed fees may be returned as NSF (non-sufficient funds). For a mid-sized restaurant, this could be thousands of dollars in fees left uncollectible by the acquirer. Risk mitigates may include daily discount, reduced processing volume or delayed funding.

- **Future delivery** – The risk with transactions dependent on the future delivery of goods and services is that the chargeback period may be quite lengthy. Examples include household furniture and/or appliances, membership dues, home renovation/remodeling, or service contracts. If the merchant goes out of business prior to delivery or completion of services and is not capable of covering the returns/chargebacks, the acquirer will absorb loss.

Anytime you have a retail establishment that you think may offer some sort of future delivery, it is important that enhanced financial due diligence be performed and ongoing audits be conducted. Examples of enhanced due diligence materials can include: an evaluation of inventory, suppliers, terms of delivery and a review of financial strength. Reserves or delayed funding may help provide financial security for future delivery merchants.

- **PIN debit transactions** – The regulations for PIN debit and the PIN debit network rules allow for cardholder disputes in certain instances. You should be aware of these regulations and understand the potential impact on your business.

- **Data security** – With the increase in merchants using point of sale systems (not just a terminal) comes an increase in the likelihood that you will experience a data breach at a retail merchant. Diligence should be used in ensuring software and hardware in use is PCI compliant and that your merchant follows proper procedures and guidelines for protecting cardholder data. If your merchant is breached and is found to be noncompliant, fines could be levied. If the merchant cannot afford to pay the fines, the acquirer/ISO is responsible. If the merchant cannot pay the fines and closes their business, non-receipt of goods/service chargebacks could become an unexpected loss to the portfolio.

- **EMV Chip Card** – If a consumer presents a chip card and the merchant is not able to accept the card AND the consumer claims fraud, the liability is now held by the merchant. This is a new risk not previously faced by card present merchants. The details of this shift are below.

  - If a merchant is not EMV certified with a chip-enabled POS terminal, and a customer pays with a chip-enabled card, then the merchant (or its acquirer) will bear the liability for any resulting fraud.
  - If the merchant is EMV ready, but the financial institution card issuer has not supplied the customer with a chip-enabled card, the financial institution card issuer will be held liable for the costs of the fraudulent transaction.
  - If the merchant is EMV certified with a chip-enabled POS terminal, and the customer pays with a chip-enabled card, and fraud still takes place, the card issuer will be liable, much like today.
### OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 5

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Counterfeit Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card</td>
<td>POS Terminal</td>
</tr>
<tr>
<td>Chip</td>
<td>Non-Chip</td>
</tr>
<tr>
<td>Non-Chip</td>
<td>Chip</td>
</tr>
<tr>
<td>Chip</td>
<td>Card Issuer is liable</td>
</tr>
<tr>
<td></td>
<td>Card Issuer has limited liability*</td>
</tr>
</tbody>
</table>

* Limited liability means that not all instances of chip-on-chip transactions will result in full financial liability on the card issuer. For instance, fallback transactions—where chip-on-chip devices are used but the transaction is not processed using chip technology—will not always result in a card issuer being liable for all costs. The acquirer or merchant must notify the issuer of the fallback transaction and the issuer will only be liable if they approve it.

**Further card brand clarification on specific fraud types and the liability shift:**

<table>
<thead>
<tr>
<th>Payment Brand</th>
<th>Transaction Type</th>
<th>Counterfeit Card Fraud</th>
<th>Lost/Stolen Card Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa</td>
<td>Chip-enabled card /Non-chip POS Terminal</td>
<td>Merchant Liable</td>
<td>Merchant Not Liable</td>
</tr>
<tr>
<td>MasterCard</td>
<td>Merchant Liable</td>
<td>Merchant Liable</td>
<td>Merchant Liable</td>
</tr>
<tr>
<td>American Express</td>
<td>Merchant Liable</td>
<td>Merchant Liable</td>
<td>Merchant Liable</td>
</tr>
</tbody>
</table>

**Authorization Data**

Along with monitoring and managing the above mentioned scenarios, the transaction data from the authorization systems provides further insight into your merchants’ processing. Utilizing information obtained during the course of the transaction, provides greater visibility into the processing activity of your merchant. Each of these data points can be used in conjunction with one another, independently, on a per transaction basis, or on an aggregate basis. These data points can further be used across like-merchant segments, across your merchant portfolio, or against metrics provided by your processor or industry standards.

- **Interchange qualification patterns/anomalies**
  - Problems with systems
  - Normal course of business
  - Merchant changing their business

- **Cardholder identification method from the terminal**
  - Swiped
  - Dipped
  - Key entered
  - Key entered with AVS
  - Key entered CNP
  - Use of the MOTO button

- **Terminal capability**
  - Swipe terminal
  - Chip/EMV enabled terminal
  - Key entered only terminal

- **Cardholder identification method**
  - Signature
  - Card present
  - AVS/CVV
Card Not Present (CNP) Transactions

Despite fraud protection tools available to merchants, in a card not present transaction, there are few instances in which an acquirer can maintain an edge over the cardholder and issuer when managing a disputed transaction.

In a retail environment the merchant can perform the following:
- Hand the physical goods directly to the cardholder
- Verify the cardholder by comparing signatures and obtaining additional forms of identification if suspicious
- Swipe or dip the card to confirm the card was present
- Readily confirm receipt of refund and exchange policies
- Obtain alternate forms of payment if not comfortable with any information presented by the cardholder

In a CNP environment, the merchant can perform the following:
- Validate card using methods such as CVV2/CVC2 and/or AVS, as opposed to a signature validation or alternate form of ID
- If the AVS or CVV2/CVC2 do not match, the merchant can ask for another form of payment or decline the transaction
- Engage the services of a third party threat validation company to review device history, validate identities, or enable knowledge-based authentication validation for high ticket items
- Enable delivery confirmation on shipped goods with signature on delivery when applicable. In the case of electronic delivery enable device tracking and IP validation rules
- Exchange and return policies should be prominently displayed or as a click-to-agree, with an email confirmation of the TOS (including the refund policy)

From a practical perspective, if the merchant does not swipe the card or read the chip, they will have less protection against actual fraudulent charges or friendly fraud. For CNP transactions, your merchant can be provided certain levels of protection against cardholder disputes, provided the merchant obtains or performs the following:
- Utilizes Verified by Visa or MasterCard Secure Code to authenticate the user at the time of the transaction. Use of this service shifts the liability for certain disputes directly to the issuer. Unfortunately, at this time, very few US merchants or issuers participate in the program. For certain merchant segments, this may be an option to mitigate the risk of cardholder fraud.
- Recurring payment transactions. In many instances, the merchant can obtain a contractual agreement with the user for recurring payments to their credit card. Agreements must be constructed to meet specific card brand criteria. Consult card brand requirements or work with your acquirer to determine exact language and benefits of such transactions. This is especially beneficial for utilities, insurance companies and institutions where the goods and services delivered are easily determined and can be validated between both parties.
Task 3: Educate merchant by applying industry best practices of card acceptance in order to prevent consumer fraud and/or chargebacks (collected or uncollected).

Objectives

This task requires that a certified professional be able to:

- Understand how the Address Verification Service (AVS) process functions;
- Outline the procedures for card present and internet based (card not present) transactions;
- Understand current prevalent fraud schemes and how to combat them; and
- Have a basic understanding of chargeback regulations including associated thresholds and potential fees.

Address Verification Service (AVS)

The Address Verification System (AVS) is a system used to verify the billing address assigned to a credit card. The system compares the credit card company’s records for the billing address of the cardholder against user input at the time of sale. Merchant providers use the AVS code to determine if there is elevated risk associated with a mismatched transaction and if further diligence is required.

Codes which cause the greatest concern are those where the merchant was unable to verify the cardholder’s address, either partial or in full.

Procedures for card present and internet based (card not present) transactions

Merchants may be involved in many types of transactions or will focus on one particular niche. Fraud prevention best practices differ by transaction types. For this exam, we will focus on card present and e-commerce (card not present) transactions.

Understanding Chargeback Risks

Payment card fraud is estimated to cost the United States $8.6 billion per year. These losses are typically taken through unfunded chargebacks. However, many small business owners have limited awareness regarding chargeback rules and subsequent fines, which are not included in the number above. Unfortunately, chargebacks are a fact of life for most businesses.

Chargebacks and Dispute Resolution

Managing chargebacks is a critical piece of a successful merchant program. An efficient and well-run merchant allows acquirers to focus on growth within their portfolio as well as process improvement. Merchants with chargeback problems create additional exposure and work for acquirers resulting in additional scrutiny of the merchant in question. Merchants with excessive chargeback problems face risk of termination and/or a cash reserve to allow their business to continue accepting credit cards. Please note that reserves should NEVER be used in place of proper merchant education and chargeback reduction. Fees and/or fines may be levied to the acquirer if their merchant exceeds acceptable chargeback thresholds as outlined by the card brands and are often passed to the merchant.

All Card Brands monitor the chargeback levels of merchants accepting their credit and debit cards. Merchants are required to keep their chargeback rates below the required thresholds, whenever excessive chargeback levels are detected, merchants and their processing banks are required to take corrective measures.

The Card Brands may impose substantial financial penalties on processing banks that fail to reduce their merchants’ excessive chargeback rates, providing another incentive to help ensure that merchants’ chargeback rates are kept within acceptable limits. Visa and MasterCard’s basic chargeback monitoring programs are listed below. Please note that there are other merchant and Acquirer level programs. Those are not covered in this section.
OVERVIEW OF TEST SPECIFICATIONS: DOMAIN 5

- **Merchant Chargeback Monitoring Program (MCMP).** MCMP monitors chargeback levels for all merchants on a monthly basis. If a merchant reaches excessive chargeback rates within month,
  - 100 sales transactions (minimum), and
  - 100 chargebacks (minimum), and
  - 1% chargeback/sales ratio in month (equal to or greater than).

Visa will notify the respective processing bank in writing. First notification of excessive chargebacks for a specific merchant is considered a warning. Visa imposes fines only if remedial actions do not result in a reduction of chargebacks (below the level listed above) within three months. Fines begin at $50 per chargeback in the 4th month and graduate up from there.

- **Excessive Chargeback Program (ECP).** The ECP monitors chargeback levels for all merchants on a monthly basis. If a merchant reaches excessive chargeback rates
  - 100 chargebacks (or more) in each of the two previous consecutive months, and
  - A ratio of chargebacks this month/sales last month of 1.50% or greater.

The acquirer must notify MasterCard in a predetermined format. Fines begin at $25 per chargeback above the 1.5% in the second month and include a fine calculated by MasterCard.

- **MasterCard has a program that does not result in fines, but does keep MasterCard informed of merchants that may cause harm to the system. A merchant becomes an Excessive Chargeback Merchant (ECM) when**
  - 100 chargebacks (or more) per calendar month, and
  - A ratio of chargebacks this month/sales last month in excess of 1.00%

This designation is maintained until the merchant is below the predetermined ratio.
Task 4: For the ISO: Maintain broad understanding and knowledge of your individual acquirer and general knowledge of their corporate risk policy and the industry’s critical factors to balance fiscal success against potential losses.

Objectives

This task requires that a certified professional be able to:

- Identify the requirements for an ISO to balance risk vs. reward for their acquiring partner; and
- Identify differences between acquirer standards for risk vs. regulatory risk.

Risk vs. Reward and a Balanced Portfolio

Understanding risk starts with an underwriting policy aligned with your corporate goals, the requirements of your acquirer and your financial strength. A start-up organization with limited capital is much less likely to have the capital fora portfolio of high risk merchants.

A balanced portfolio is a portfolio that is not heavily dependent upon one industry type or a few select merchants or cyclical businesses. Comparing the portfolio of your organization against industry metrics is a good way to establish a baseline and determine best practices. Items to use in the process of building your portfolio strategy include:

- Average merchant size
- Merchant profitability
- Portfolio profitability
- Transaction counts
- Chargeback ratios
- Refund percentages
- Card not present vs. face-to-face processing
- Future delivery of goods or services
- Digital content
- Registered high-risk merchants
- Acquirer reserves on file
- Merchant industry (MCC) analytics
- Merchant reserves
- Fraud tools used by CNP merchants
- Compensation strategy for your sales reps
- Underwriting or evaluation of sales reps

Using these and other parameters at the merchant, agent and portfolio levels as guidelines, you can work to determine the appropriate merchant mix for your risk appetite and that of your acquirer. Your written policies should clearly outline your goals and your procedures must support those policies. Periodic evaluation of your portfolio and adjustments to your strategy should be a standard business practice.

Acquirer Standards vs. Regulatory Risk

Your acquirer will be clear about their requirements and the risks they believe should be mitigated. To be a conscientious industry participant it is important to also pay attention to the regulatory risk currently engulfing this industry. Currently the DOJ, CFPB and FTC are taking a long hard look at the payments processing industry. They all see this industry as a gateway to consumer harm. It is very important that we understand this and work to protect the cardholders/consumers from harm. We can do this by understanding our merchants and ensuring that they provide the service and/or product as advertised.
DOMAIN 6: REGULATORY/COMPLIANCE/SECURITY

Task 1: Acquire and maintain current knowledge of appropriate/available regulations governing the payments processing industry through trade organizations, card brands, media, networking, magazines, online resources, etc. in order to educate merchants and ensure compliance by the sales agent, consumer, and merchant.

Objectives

This task requires that a certified payments professional be able to:

■ Study and maintain working knowledge of payment regulations;
■ Understand regulatory compliance effects on merchant processing;
■ Attend annual training at a minimum to stay current with trends and interpretations; and
■ Understand the scope and terms of all regulations, including but not limited to which merchants fall under which regulations and which version of the regulations is current.

▲ Organizations in the United States must comply with numerous regulations based on their vertical market and the size of the organization. These organizations must maintain knowledge of all current versions of the various regulations. The primary overseers that govern credit card acceptance are the card brands (Visa, MasterCard, American Express and Discover). Collectively the brands set the minimum acceptable use standards for global card acceptance. Secondary governors of the payments ecosystem are various USA federal regulators ex: OCC, FDIC, FFIEC, CFPB or the FTC. The Payment Card Industry (PCI) standards apply when an entity comes into contact with Primary Account Number (PAN).

▲ Updates to regulations will increase the compliance burden for the companies that are required to comply with those regulations. A comprehensive understanding of what and how changes will impact them and their constitutions must be attained prior to release. An example is the PCI DSS 3333.0 clause which stated that a merchant must prove that cardholder data does not reside in areas which are stated to be outside of the cardholder data environment (CDE). This became a mandatory requirement that affects you and the merchant.

▲ Many regulatory bodies offer conferences to clarify their positions, explain the intent of regulations, and to offer suggestions to the board. Regular attendance of these events or training within the organization by a qualified individual should be scheduled to keep all critical personnel up to date with changes and trends in the industry and the governing body’s interpretations of their regulations.

▲ You must be familiar with the purpose of each major regulatory body, as well as understand which businesses must comply with each (e.g., SOX applies only to SEC registrant companies). In addition some regulations are updated regularly and you should be aware of these scheduled updates and anticipate spending time getting familiar with them. You must maintain a working knowledge of the changing regulations, such as new requirements or recommendations set forth in PCI DSS updates. In some cases changes to regulatory requirements take effect on specific dates. You should be familiar with these timeframes and keep track of the important dates when each major change occurs and any grace periods in the regulations.

▲ While compliance regulations are a good place to start with regard to securing payment channels, they are generally considered “security minimums,” and as such may not protect the business adequately. A basic understanding of information security best practices, such as encryption and tokenization, is essential to keep businesses up and running.

▲ Maintain a working knowledge of third party risk mitigation, as well as the card brand specific approved service provider listings. Remember, in the payments system each entity is responsible, regardless of contractual agreements, for the actions of their 3rd parties. For example, a bank that contracts with an ISO must ensure the ISO performs all duties within the boundaries of the card brands’ regulations as well as the various governmental organizations mentioned previously.

*See references for Domain 6
Task 2: Educate merchant base on all applicable regulations, impact of non-compliance, and how to comply by presenting merchants with verbal and written materials to avoid sanctions and/or possible fines or regulatory action.

Objectives

This task requires that a certified payments professional be able to:

Present regulations in an organized manner:
- Explain the intent and business benefit of regulations and best security and regulatory practices;
- Collect and maintain a comprehensive library of materials to distribute to merchants; and
- Assist merchant in closing security or compliance gaps between their current environment/operations and current regulations.

▲ You must be able to present regulations in a clear and organized manner to the merchant. Be aware of the major sections of the regulations and how they apply to merchants. Keep in mind most merchants are not experts on payment and other governmental regulation compliance and need to be educated. Organization is the key to successful processes around compliance, so the merchant will turn to you as the subject matter expert providing them a blueprint for meeting regulations.

▲ Most regulatory bodies leave the exact implementation of the regulations up to the assessor and/or the organization itself. Understanding the intent of each regulation will allow you to provide the merchant with a more economical and efficient way of reaching their security or compliance goals. Often a small amount of additional process or training can replace an expensive off-the-shelf product or application.

▲ Be a warehouse of relevant information and materials to merchants. Be aware of which documents are relevant to which merchants. For example, a PCI Level 4 merchant does not need to undergo an onsite audit, so a Self Assessment Questionnaire (SAQ) would be appropriate based on the type of business they do (and as defined by the acquirer). Another example would be validating that a telemarketing merchant is compliant with the recent Telemarketing Sales Rule (TSR) amendments.

▲ Merchants may have a limited knowledge of information security fundamentals that will assist them in meeting industry regulations or good business practices. You should be able to provide the merchant with guidance on strategies and technologies based on their business type that can help them close the gap between their current environment/operations and what they’ll need to do to be compliant and secure. Although you should never recommend any specific product, you can introduce the merchant to a family of industry approved third party services, which may be able to assist them.*

*See references for Domain 6

Task 3: Gather proper documentation from merchant to make sure merchants are compliant with all regulations.

Objectives

This task requires that a certified payments professional be able to:

- Apply relevant regulations to merchant environment; and
- Collect documentation in support of applicable regulations.

▲ You should be able to determine the regulations relevant to a particular merchant’s cardholder data and overall regulatory environment and the merchant’s responsibility to those regulations. This includes the processing, storage and transmission of sensitive information, physical security, network security, monitoring, consumer harm protocol, licensing requirements based on vertical, proper policies and procedures, and the auditing and testing of all relevant elements.
The merchant is responsible for providing all applicable documentation. They may have questions about how to prove various aspects of compliance to an auditor or assessor. You should be able to make suggestions on how to document various things such as quarterly network scans, access controls, security policies, disaster recovery, return policies, sales scripts, and any other relevant procedures. Examples of allowed documentation include screenshots of various applications, firewall access control lists, text dumps of user and group files, sales scripts, return policy documentation, endorsement contracts, and most importantly process or policy documents that represent your business philosophies and practices.

**Task 4: Inform merchants of all consumer protection, data management, security, and storage regulations and best practices to ensure compliance by all stakeholders.**

**Objectives**

This task requires that a certified payments professional be able to:

- Understand storage and transport mechanisms including the advantages and disadvantages of each.

> Ultimately most payments regulations are created to help safeguard and protect the consumer from harm and the loss of their sensitive data. For example in the health care field (including doctors, clinics, psychologists, dentists, chiropractors, nursing homes or pharmacies) that would mean the safe acquisition, transmission or storage of Protected Health Information (PHI), which includes payment methods. For an e-commerce widget seller site it is customer credit (PAN) and personally identifiable information (PII). Personal Information is defined as individual’s first name or first initial and last name plus one or more of the following data elements:

- Social Security number,
- Driver’s license number or state issued ID card number,
- Account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Consult with your counsel if protected data is compromised, there are various state and federal notification requirements. Create an environment of trust with your merchants so they will escalate breaches and ask for help, rather than trying to navigate the waters alone.

> The regulators define acceptable customer engagement models/methods then test and measure their success. The goal is to protect consumers from false or misleading claims in the advertising. Further information about Unfair, Deceptive, and Abusive Acts or Practices (UDAAP) can be found in the Dodd Frank Act. A bank, ISO, PF, and merchant are all responsible for protecting the consumer and any data they collect regardless of whether it is in-flight or at-rest. You must be familiar with technologies which protect data while it is in-flight such as SSL, TLS, and VPN, and technologies which protect data at-rest such as encryption, segmentation, tokenization, access controls, and even written policies. Following industry best practices will often set the merchant above the bar for various regulations; so encouraging merchants to do so will often significantly lessen their level of effort for compliance each year.
Sample Questions – Domain 1

1. Which of the following is a standard method to group prospective leads?
   a. Square footage of business
   b. Number of items for sale on their website
   c. Geographic location
   d. Political affiliation

2. Which of the following is the LEAST effective method of developing a list of prospects?
   a. Research the industry
   b. Talk to local influencers
   c. Consider the product set of their business
   d. Cold call on initial prospects of interest

3. Which of the following is NOT a part of the consultative sales approach?
   a. Aggressive telephone calls
   b. Active listening
   c. Understanding closing techniques
   d. Effective closing strategies

4. In addition to features and advantages, traditional product positioning includes which of the following?
   a. Cost
   b. Units deployed
   c. Benefits
   d. Competition

5. When first meeting a prospect, which of these activities might a sales professional engage in to ease tension?
   a. Purchasing their product
   b. Presenting the proposal
   c. Open ended questions
   d. Closed ended questions

6. Active listening is best supported by which of the following activities when on a sales call?
   a. Follow up questions
   b. Advancing the sale
   c. Problem resolution
   d. Objection handling

7. Which of the following is the most appropriate response when a merchant objects to a particular solution being offered?
   a. Stop and listen
   b. Immediately offer another solution
   c. Lower the price
   d. Quickly explain the benefits

8. Excellent sales people best prepare for objections by doing which of the following?
   a. Offering your best price first
   b. Anticipating objections prior to the call
   c. Continually closing
   d. Moving the conversation or presentation faster

9. Which of the following is the largest negotiation element in any sales call?
   a. Price
   b. Value
   c. Service
   d. Length of term

10. Which of the following is the BEST method of selling value over price?
    a. The return on investment of the product or service being sold to the customer
    b. The detailed plan for implementation of the product or services being sold to the customer
    c. The price being paid by the merchant today
    d. Understanding the competition’s product in place at the customer
11. Which of the following methods is NOT appropriate for contract execution?
   a. Actual signature from the owner in ink on the application
   b. An electronic signature by the owner
   c. A signed letter on letterhead, of acceptance from the owner
   d. A signed and faxed application from the owner

12. Which of the following is NOT part of the ongoing sales support function?
   a. Timely response
   b. Accurate record keeping
   c. Basic technical understanding
   d. Detailed technical knowledge

13. Which of the following is NOT an accurate source for industry knowledge?
   a. VISA, MasterCard, American Express and Discover websites
   b. Electronic Transactions Association website
   c. Wikipedia
   d. Federal Trade Commission website

14. In the United States, which organization is responsible for creation and administration of the merchant contract?
   a. The card brands
   b. The acquiring bank
   c. The ISO
   d. The sales agent

15. In the United States, a merchant services contract is between a merchant and which of the following?
   a. The card brands
   b. The ISO
   c. The acquiring bank
   d. The sales agent

Sample Questions – Domain 2

1. What data elements are required for a merchant’s commercial card transactions to qualify for Level 1, Level 2 and Level 3 Interchange programs?
   a. Account #, address and zip code
   b. Item #, date and AVS Info
   c. Customer #, order #, CVV #
   d. Customer #, sales tax and invoice #

2. What types of transactions and which banks were regulated by the Durbin amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act?
   a. Swiped transactions from foreign banks
   b. Corporate card transactions from issuing banks
   c. Regulated debit card transactions from large issuing banks
   d. MOTO check cards from domestic banks

3. What constitutes a small ticket transaction?
   a. Sales less than $25.00
   b. Internet transactions under $10.00
   c. Recurring billing transactions under $50.00
   d. Swiped sales under $15.00

4. What does EIRF stand for?
   a. Transactions captured electronically
   b. Electronic transactions captured and settled within 2 days of authorization
   c. Transactions captured and settled within 29 days of authorization
   d. Transactions captured on a corporate or international card

5. What is the Interchange rate charged for transactions that clear for EIRF?
   a. 1.54% + $.10
   b. 2.70% + $.10
   c. 2.30% + $.10
   d. 1.85% + $.10
6. How is a merchant’s effective rate calculated?
   a. Discount rate x average ticket
   b. Sum of Qualified, Mid- and Non-Qualified fees
   c. Total fees divided by total sales
   d. Number of transactions x transaction fee

7. What does surcharge/bill back mean on a merchant’s statement?
   a. Mid and Non-Qualified fees
   b. Total sales
   c. Monthly processing fee
   d. Discount rate

8. On a merchant statement, how would you determine if the merchant is being billed on Interchange Plus, tiered pricing or a bundled rate program?
   a. Look at the discount rates section
   b. Add up all transaction fees
   c. Calculate non-qualified fees
   d. Look at all monthly fees

9. How can a merchant’s charge per authorization be determined when the amount appearing on the statement is the total for all authorizations?
   a. Add up all the fees and divide by sales volume
   b. Total sales divided by average ticket
   c. Authorization fees divided by number of transactions for each card type
   d. Discount fees divided by average ticket

10. How would a $79 annual fee get converted into basis points (bps), for a merchant that processes $10,000 a month in sales volume?
    a. Divide 79 by 10,000 x 12
    b. Divide 79 by 12 and divide by monthly sales
    c. Multiply 79 by 12 months, then divide by 10,000
    d. Multiply 79 by the discount rate

11. Which of the following is a benefit to pricing a merchant on an Interchange Plus program verses a tiered rate program?
    a. Full cost disclosure
    b. More detailed volume reporting
    c. Mid and Non-Qualified fees are detailed
    d. Flat rate for all fees

12. What is tiered pricing?
    a. Processing fees charged at different volume tiers
    b. Interchange rates grouped into major categories for simpler pricing
    c. Swiped, non-swiped and debit fee totals
    d. Processing fees charged by card type

13. Which one of the following would use a Micros terminal?
    a. An e-commerce merchant
    b. A wireless merchant
    c. An international merchant
    d. A restaurant merchant

14. What is host capture?
    a. Authorized transactions are captured on approval and settled on processors system
    b. The definition for an Internet gateway used by e-commerce merchants
    c. How ATM debit and EBT transactions are processed
    d. Terminal stores approved transaction in batch for settlement at days end

15. What is terminal capture?
    a. POS device authorizes each card type and sends approval to merchant
    b. Transaction approved by processor then captured in memory in terminal for batch settlement
    c. Terminal is downloaded for all merchant processing parameters
    d. POS transaction is swiped and authorized electronically
SAMPLE EXAMINATION QUESTIONS

16. What is a gateway?
   a. Software needed to connect POS devices and peripherals together
   b. The connection between the host processor and terminal at the merchant site
   c. A web-based virtual terminal that connects to major processors for browser based and e-commerce transactions
   d. Name for merchant’s front end processing platform

17. What purpose does a gateway serve for a merchant?
   a. To process transactions originating from a website or shopping cart
   b. To use a POS terminal over the Internet or WIFI network
   c. To connect to a new processor network and control fraud
   d. To convert from a dialup to an internet based terminal

Sample Questions – Domain 3

1. What is the correct term for a number used to identify the merchant during processing of daily transactions, rejects, adjustments, chargebacks, and end-of-month processing fees?
   a. Terminal Identification Number
   b. Automated Clearing House Number
   c. Merchant Identification Number
   d. Demand Deposit Account Number

2. What is the most efficient way for a merchant to process other than via a phone line?
   a. A laptop
   b. IP or ethernet processing
   c. Fax
   d. Voice authorization

3. What is the best method to communicate with a merchant?
   a. Text
   b. Facebook
   c. Leave a note on their account
   d. Email

4. Which one of the following relationships is NOT important to the success of retaining a merchant account?
   a. Customer service
   b. Mail carrier
   c. Risk management
   d. Technical support

5. Which of the following is NOT an important component of a merchant processing statement?
   a. Header information
   b. Deposit summary
   c. Surcharges
   d. Tips on how to save money

6. Which of the following methods of processing uses a secure web server that provides an interface for merchant websites and shopping carts that require real-time transaction processing?
   a. Mobile solutions
   b. Landline terminal
   c. Wireless terminal
   d. Internet solutions

7. Which of the following peripheral devices reads pocket-sized cards with embedded integrated circuits that can process and store data, and communicate with a terminal via radio waves?
   a. Landline terminal
   b. Pin pad
   c. Contactless reader
   d. Check reader

8. What term best describes the accumulation of captured credit card transactions in the merchant’s terminal or POS system awaiting settlement?
   a. Batch
   b. Credit
   c. Deposit
   d. Processing
9. Which entity typically initiates a chargeback?
   a. Acquirer
   b. Card issuer
   c. Cardholder
   d. Merchant bank

Sample Questions – Domain 4

1. What type of questions should you ask a merchant to have them provide a detailed explanation of their business objectives and needs for credit/debit card processing?
   a. What payment types and ancillary services are needed?
   b. What advertisers do you use?
   c. How do you price your products?
   d. How many student employees do you have?

2. What is the one ‘key’ question to ask, when considering the impact of a potential payments solution for a merchant that has 90% face-to-face transactions, and 10% MOTO transactions with one stand-alone dial terminal currently in place?
   a. Do you have in-house IT staff available?
   b. Do you accept checks as a form of payment?
   c. How many face-to-face credit card transactions do you process per hour?
   d. What percentage of credit card transactions are taken over the telephone versus taken via email?

3. Which of the following is part of the process for training/educating a merchant on the use of a terminal?
   a. Test the terminal and provide merchant with technical support number (usually an 800 number)
   b. Read the terminal user guide to the merchant
   c. Include a DIY (do it yourself) guide in the box with the terminal
   d. Provide the merchant with the terminal manufacturer phone number

4. What is the first step that leads into the discussion of payment mechanisms, ancillary solutions required by the merchant, and any additional data exchange as part of the payment process or apart from the payment process?
   a. Gift card processing, including support for an existing gift card program
   b. Determine merchant need or desire to accept primary payment brands
   c. Need for purchasing card support, including level 2 or level 3 data
   d. Check verification, guarantee, or Check 21

5. What does “No Line” mean when displayed on the POS device?
   a. No lines will print on the receipt
   b. No waiting in line
   c. No dial tone detected
   d. No power

6. A chip card performs which of the following functions?
   A. Encrypts the magnetic stripe for transmission over the telecom lines
   B. Encrypts the magnetic stripe prior to passing it into the terminal
   C. Utilizes an algorithm to send to the issuer instead of track data
   D. Utilizes an algorithm to encrypt data off of the magnetic stripe

7. End-to-End encryption is best described as:
   a. card data encrypted within the magnetic stripe reader environment and remaining encrypted all the way to the processor’s host or card brand
   b. Card data encrypted in the terminal by software, just prior to passing the card data onto the network to the gateway
   c. Card data encrypted within the magnetic stripe reader and within the keypad (for key entered transactions) and remaining encrypted all the way to the processor’s host or card brand
   d. A mandate by the card brands that all equipment and processors must support
8. Tokenization is best described as:
   a. Encrypting card data for recurring billing purposes
   b. Providing a merchant or system with a value that corresponds to card data for use in transaction processing
   c. Providing a user with encrypted card data for use in transaction processing
   d. Something that the merchant does with their database prior to sending to the card issuers

9. How many tracks of data are encoded on a standard credit card?
   a. 1
   b. 2
   c. 3
   d. 4

10. Which of the following is applicable to a gateway provider?
    a. They always connect directly to the card brands
    b. They connect to the payments processors
    c. They are not regulated by the card brands
    d. They must support all card types and brands

Sample Questions – Domain 5

1. Which of the following merchant types would be placed under permitted? (Some merchant types could fit under more than one category)
   a. Adult content
   b. “Knock off” goods
   c. Lingerie sales
   d. Gambling

2. Which of the following merchant types would be placed under Restricted? (Some merchant types could fit under more than one category)
   a. Makeup sales
   b. Tobacco
   c. Neutraceuticals
   d. Trophy Shops

3. According to the MasterCard and Visa rules, which of the following types of merchants would be required to be registered in the high risk category?
   a. Drug stores and pharmacies
   b. Counterfeit and copyright infringement merchandise
   c. Deceptive marketing practices
   d. Illegal prescription drugs

4. What is the purpose of AVS?
   a. To assist in the verification of the cardholder both on and offline
   b. To guarantee the transaction
   c. A decline code
   d. To verify the mag stripe

5. Which of the following IS NOT a card present best practice?
   a. Swipe the card
   b. Ignore the card expiration date
   c. Check authorization response
   d. Obtain a signature

6. Which of the following IS NOT a card present warning sign?
   a. Purchases for groceries and standard household items
   b. Cardholders making larger ticket purchases than approved during UW
   c. Purchases at unusual hours
   d. Purchases of large quantities of items that are out of pattern

7. Which of the following is NOT a warning sign of e-commerce (Card Not Present) fraud?
   a. Orders on multiple credit cards
   b. Shipping to an international address
   c. Multiple transactions on one card over a short period of time
   d. Repeat customer with good history
8. Which of the following is NOT a merchant initiated type of payment card fraud?
   a. Bust out
   b. Collusion
   c. Shipping goods when CVV doesn’t match
   d. Factoring

9. Which of the following is a trigger that will place a merchant on a Card Brand Chargeback Monitoring Program?
   a. Chargeback rates less than 1%
   b. Number of chargebacks is equal to the number of sales in one day
   c. Chargeback rates greater than 1.5%
   d. Chargeback is 50% greater than average ticket

10. Which of the following represents a balanced portfolio?
    a. A portfolio that does not cause losses
    b. A portfolio that is not reliant on any one segment or a small set of merchants.
    c. A portfolio that is approved by the acquirer
    d. A shared BIN portfolio

11. Which regulatory agency is NOT currently a factor in acquiring?
    a. DOJ
    b. FTC
    c. OSHA
    d. CFPB

12. In which situation below is the merchant liable?
    a. Mag stripe only card swiped at the point of sale cardholder claims fraud.
    b. Chip card dipped in the terminal and the cardholder claims fraud.
    c. Chip card not dipped and it is counterfeit fraud.
    d. Visa chip card swiped and not dipped cardholder claims lost or stolen.

13. Merchants with chargeback problems tend to be:
    a. Ok because there is a fee earned by the provider for each chargeback
    b. Ok if reserves are in place to cover them
    c. Ok as long as the merchant is educated about the chargeback process
    d. Exhaustive of resources and causes additional exposure for acquirers

14. In a CNP environment the following is NOT a protective measure for the merchant:
    a. Engage the services of a third party threat validation company to validate identities.
    b. Obtain a signed authorization form in place of non-matching AVS.
    c. Display a click to agree with e-mail confirmation for online exchange and return policies.
    d. Enable delivery confirmation of shipped goods.

15. Future delivery of goods and services provided by a merchant:
    a. Allows merchants to obtain funds up front to purchase product.
    b. Only matters when the merchant goes out of business.
    c. Only matters if the merchant is CNP.
    d. Extends the chargeback period.

16. What data elements won’t be able to help you ascertain the risk balance of a portfolio?
    a. MCC concentrations
    b. % of registered high risk
    c. CNP ratio to CP
    d. Terminal type

17. Which answer is not true: Repeat or excessive auths could be a sign of:
    a. Technical issues
    b. Customer confusion/excitement
    c. Auth testing
    d. A sale
18. When is it permissible to change the MCC
   a. When the merchants primary line of business changes
   b. When changing it will enable more authorizations to clear
   c. After the merchant complains about down grades
   d. To evade registration requirements

19. How soon after you get notified about a problematic chargeback merchant should you close the account and open up a new one?
   a. 15 days
   b. 20 days
   c. Immediately
   d. Never

20. When a merchant is facing challenges with chargebacks should you:
   a. Increase their reserves to cover your potential fine exposure
   b. Increase their monthly volume to offset the disputes
   c. Help the merchant open multiple accounts to load balance
   d. Launch a fact finding mission and tailor an education campaign based on learnings

Sample Questions – Domain 6

1. Credit card track data stored on a hard disk drive is considered:
   a. In-flight
   b. Out of scope
   c. At-rest
   d. Encrypted

2. An auditor can accept all of the following forms of evidence to prove compliance EXCEPT:
   a. Employee’s word
   b. Configuration files
   c. Official company policies
   d. Screenshots

3. PCI Compliance is mandatory for merchants accepting what volume of credit card transactions annually?
   a. Less than 1 million transactions annually
   b. From 1 million to 6 million transactions annually
   c. More than 6 million transactions annually
   d. All merchants regardless of size must be compliant if they accept credit cards

4. Where can specific UDAAP regulations be found?
   a. The Dodd Frank Act.
   b. The OCC Guidelines
   c. The Telemarketing Sales Rule
   d. Visa and MasterCard regulations.

5. Sarbanes Oxley applies ONLY to:
   a. Companies with over 1000 employees
   b. SEC registrant companies
   c. Companies accepting credit or debit cards for purchases
   d. Health care organizations

6. In PCI DSS an SAQ is a:
   a. Single Account Quota
   b. Self Assessment Questionnaire
   c. Security Assessment Questionnaire
   d. Security Applicability Quiz

7. VISA, MasterCard, American Express, and Discover are referred to as:
   a. Payments processors
   b. Payment card brands
   c. Merchants
   d. PCI SSC

8. PCI Merchant levels are determined by a merchant’s:
   a. Number of employees
   b. Annual transaction processing dollars
   c. number of transactions processed
   d. Previous year’s merchant level
9. Payment card security is concerned with protecting all of the following types of data EXCEPT:
   a. Primary Account Number (PAN)
   b. Sensitive Authentication Data (SAD) like CVV
   c. Card Track Data
   d. Social Security Number

10. An annual Self-Assessment Questionnaire, and scanning if applicable, in lieu of an onsite audit, is acceptable for all of the following merchant levels EXCEPT:
    a. Level 1
    b. Level 2
    c. Level 3
    d. Level 4

11. In the case of a potential data breach, the merchant is required to:
    a. Follow their incident response plan
    b. Immediately email the card brands
    c. Print out a list of all cards that may have been compromised.
    d. Call the local FBI office

12. Which one below is not PII?
    a. Social Security Number
    b. Driver's License Number
    c. Home Address
    d. Latitude and Longitude
## SAMPLE EXAMINATION QUESTION ANSWER KEY

<table>
<thead>
<tr>
<th>QUESTION #</th>
<th>DOMAIN 1</th>
<th>DOMAIN 2</th>
<th>DOMAIN 3</th>
<th>DOMAIN 4</th>
<th>DOMAIN 5</th>
<th>DOMAIN 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C</td>
<td>B</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>2</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>C</td>
<td>C</td>
<td>A</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>4</td>
<td>C</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>5</td>
<td>C</td>
<td>C</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>6</td>
<td>A</td>
<td>C</td>
<td>D</td>
<td>C</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>7</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>A</td>
<td>D</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>B</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>10</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>11</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>D</td>
<td>C</td>
<td>A</td>
</tr>
<tr>
<td>12</td>
<td>D</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>C</td>
<td>D</td>
<td>D</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>C</td>
<td>B</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>C</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>A</td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REFERENCE MATERIAL AND ADDITIONAL RESOURCES

The following reference material can help you prepare for the Certified Payments Professional exam

General References

**ETA:**
- ETA University Courses: http://www.electran.org/content/category/9/99/206/
- ETA conferences and events – www.electran.org

**Industry-related websites, meetings, publications and regular email blast updates**
- Digital Transactions news - http://digitaltransactions.net

**Industry-related local and chapter meetings and networking events**

**Card Brands:**
- best practices
- requirements and standards
- websites
- offerings and newsletters

Reference Material – Domain 1

**Company resources:**
- Corporate sales policy manuals
- Corporate sales training materials
- product manuals and service offering training
- Corporate standards and policies on contract execution
- Corporate standards for client interface and support after the sale
- SFA CRM solution
- Corporate documentation and contract processes and procedures (steps)
- Acquirer implementation guide
- Corporate IT department for technical product offerings and training
- Corporate selling kit and model describing the FAB of the company to the industry
- **Current client list** – for thoughts on areas of expertise or focus
- **Current prospect lists** – for local businesses or by segment that the company has solicited in the past
- **Active listening** –

- **Book on customer service** –

58 ETA CPP: EXAMINATION STUDY GUIDE © 2016 ELECTRONIC TRANSACTIONS ASSOCIATION
REFERENCE MATERIAL AND ADDITIONAL RESOURCES

- The Book of the Five Rings –
  http://www.amazon.com/Book-Five-Rings-Miyamoto-Musashi/dp/1590308913/ref=sr_1_1?ie=UTF8&qid=1322801450&sr=1-1

- Cold calling techniques –
  http://www.amazon.com/Smart-Calling-Eliminate-Failure-Rejection/dp/0470567023/ref=sr_1_1?ie=UTF8&qid=1322800386&sr=1-1

- Customer service website –
  http://www.customerservicemanager.com/

- Feature Advantage Benefit (FAB) –
  http://www.amazon.com/Long-Tail-Revised-Updated-Business/dp/1401309666/ref=pd_sim_b_1

- Fish –
  - http://www.amazon.com/Remarkable-Boost-Morale-Improve-Results/dp/0786866020/ref=pd_sim_b_5

- Getting to Yes –
  http://www.amazon.com/Getting-Yes-Negotiating-Agreement-Without/dp/0143118757/ref=sr_1_1?ie=UTF8&qid=1322801167&sr=1-1

- Goldmine – http://www.frontrange.com/ - website / software $$$


ISO implementation process requirements

- ISO & Agent publication – www.isoandagent.com


- Negotiating the Complex Sale – http://www.amazon.com/SPIN-Selling-Fieldbook-Practical-Exercises/dp/0070522359/ref=pd_cp_b_1


- Salesforce.com – www.salesforce.com – website / software $%

- Selling Power magazine – www.sellingpower.com


- www.speconline.org/cppg
Reference Material – Domain 2

- Ask your company’s sales department for copies of merchants’ statements from the various processors/acquirers

Reference Material – Domain 3

- http://www.merchantcouncil.org/
- http://www.100best-merchant-accounts.com/terms/
- Merchant Accounts; If You Want To Learn About Merchant Accounts, Get This Guide About Merchant Services, Credit Card Processing, Retail Merchant Accounts, Visa Merchant Accounts, And Much More! eBook Michael M. Bennett (Author)
- http://www.checktraining.com
- http://en.wikipedia.org/wiki/Credit_card
- http://en.wikipedia.org/wiki/Payment_card_industry

Reference Material – Domain 4

- Access chosen processor solution’s website and view the merchant solutions area
- Account management
- Check verification and guarantee solutions
- Customer service at the processor
- Gift card processing solutions
- Hardware solutions for credit and debit support
  - www.verifone.com
  - www.equinox.us
  - www.ingenico.us
- Other sales reps
- Training classes provided by the processor
- User guides and training materials on the various solutions
- Visa’s NAICS list of merchant category codes
Reference Material – Domain 5

- Card brand operating regulations
- Interchange charts
- Regulations Z & E
- Processor tools such as risk reporting and data specifications
- http://broadcast01p.visabroadcasts.com/xfm/?5988/0/6239a0b1461cc6d1d410dfccff2a6b0a/16778824

<table>
<thead>
<tr>
<th>Code</th>
<th>Summary</th>
<th>Value Description</th>
<th>Visa</th>
<th>MC</th>
<th>AMEX</th>
<th>DISC</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Match</td>
<td>Street address and 9-digit ZIP code both match</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Y</td>
<td>Match</td>
<td>Street address and 5-digit ZIP code both match</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>A</td>
<td>Partial Match</td>
<td>Street address matches, but both 5-digit and 9-digit ZIP Code do not match</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>W</td>
<td>Partial Match</td>
<td>Street address does not match, but 9-digit ZIP code matches</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Z</td>
<td>Partial Match</td>
<td>Street address does not match, but 5-digit ZIP code matches</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>N</td>
<td>No Match</td>
<td>Street address, 5-digit ZIP code, and 9-digit ZIP code all do not match</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>U</td>
<td>System Unavailable</td>
<td>Address information unavailable. Returned if non-US. AVS is not available or if the AVS in a U.S. bank is not functioning properly.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>R</td>
<td>System Unavailable</td>
<td>Retry - Issuer's System Unavailable or Timed Out.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Invalid</td>
<td>AVS data is invalid</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>Not Supported</td>
<td>U.S. issuing bank does not support AVS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>


Notated below are resources that can provide guidance on loss prevention, underwriting and general industry compliance. Additionally, links have been provided for reporting fraud to all of the major card brands.
GENERAL INDUSTRY COMPLIANCE

- **Internet Web Services**
  there are a number of companies who provide a wide range of services to help monitor your various relationships. These entities offer solutions to protect companies from brand-damaging and/or illegal transactions.

- **Merchant Acquirers’ Committee (MAC)**
  (https://www.macmember.org/) – MAC is a broad-based organization of bankcard risk professionals. Through their email alerts, various stakeholders within our community are able to share information in a timely manner. Visit the website for additional information and how to become a member.

- **BinBase Project**
  (http://www.binbase.com/search.html) – Although not supported by any of the card schemes, the BinBase project can also provide some useful insight. They currently have 140,000+ BIN records on file. This information can provide initial guidance on which banks you should contact if you come across a problem.

- **ACH Payments**
  (http://achprocessing.typepad.com/ach_processing/2005/12/ach_nacha_retur.html) – An additional common problem facing our industry surrounds ACH rejects, with the most common question being What do the rejection codes mean? Additional information on the ACH Processing Solutions can be found at http://www.achpayments.com/.

- **Web Hosting Talk**
  (http://www.webhostingtalk.com/) – A great resource to monitor the webhosting guys

GOVERNMENT AGENCIES

When it comes to risk, we all need to be aware of how our industry intertwines with various government agencies. Two of the main agencies are:

- **The Federal Trade Commission**
  (http://www.ftc.gov/) – We have all seen a recent uptick in the FTC’s involvement in investigating different merchant segments. It’s safe to say that we would rather work with them to ensure the stability of the payment system as to working against them, which in the short run may increase your bottom line, but in the long run may result in something as disastrous as your business being shut down.

- **The Federal Communications Commission**
  (http://www.fcc.gov/)

- **Secretary of State websites**
  The Secretary of State department registers and issues business licenses in most states. Each business that you are working with should have an official notification from their applicable Secretary of State. Additionally, many Secretary of State offices also have information on trademarks and service marks issued in their jurisdiction. As we see an increase in legislation surrounding trademark and copyright infringement, it is important to know where to look to find an authoritative source.

UNDERWRITING OR MONITORING RESEARCH

Finally, when doing underwriting or monitoring research you should always look to the sites listed below. While you may not find the whole story on any one entity, using the different puzzle pieces that are gained from each can be invaluable.

- **Better Business Bureau (BBB)** (www.bbb.com) – This group focuses on ensuring consumers have access to information relating to businesses within the United States. This can often be used as a front line tool to determine if a business you are potentially going to work with has any consumer reported issues.

- **Facebook** (www.facebook.com) and **LinkedIn** (www.linkedin.com) – While these social networking sites generally don’t have consumer information, they can be used for verification of a person’s location. Users often note where they are from or where they currently live, so when reviewing an application you can verify the application details by using these two tools.
REFERENCE MATERIAL AND ADDITIONAL RESOURCES

- **Go Daddy** (Godaddy.com) – This site is one of the largest domain name registrars and hosting providers. They offer a variety of services which can assist in underwriting a merchant.

- **Google** (www.google.com) – This search engine is one of the best free tools for our industry that is often underutilized. When underwriting a new merchant or agent, a basic search will reveal if the company you are doing business with has any complaints against them and whether or not there is any background info you were not provided as part of the underwriting. Additionally, Google can be used as a base tool to verify the physical address of the merchant/agent for those times and locations where doing an on-site visit is not possible or necessary.

- **IP Lookup** (http://ip-lookup.net/) – This site will help determine if the merchant you are working with truly resides where their application says they do by tracing their IP address. For instance, if your merchant notates that they are based out of Oregon, but their IP address lists Cyprus, you can bet you have a problem that should be further investigated.

- **Ripoff Report** (www.ripoffreport.com) – This consumer reporting tool can be useful to identify merchants and agents who have had numerous consumer complaints.

- **Whois-search.com**
  This site will allow you to note who is associated with a particular website address. This is useful when you are trying to determine the true owner of a website and when the website was first set up.

- **Zillow** (www.zillow.com) – This tool provides information geared towards home prices. If a merchant or agent lists its home as an asset you can use this site to verify its current value.

ADDITIONAL INFORMATION/RESOURCES

In addition to the above mentioned resources, everyone in the industry should be aware of The Green Sheet (http://www.greensheet.com/) and Transaction Trends (the official publication of the ETA). These two publications provide timely articles as well industry contacts.

Finally, as you attend conferences, meetings or other industry events remember to develop and keep those contacts. Although the person you know may not have the answer, they will often be able to help point you to someone who does.

As always if you believe you are experiencing fraud you should immediately reach out to the various card schemes and appropriate authorities to report the incident. You can do so by e-mailing the appropriate contact at the emails noted below.

- **Visa**
  USFraudControl@visa.com

- **American Express**
  AMEX.Fraud.Solutions@aexp.com

- **Discover**
  dnfraud@discover.com

- **Diners Club**
  dcifraud@discover.com
Reference Material – Domain 6

Data Security
- EMVCo, www.emvco.com
- P2PE, wikipedia.org/wiki/Point_to_Point_Encryption
- Validated P2PE Solutions, pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php
- E2EE, wikipedia.org/wiki/End-to-end_encryption

Security Best Practices
- Intrusion detection system, wikipedia.org/wiki/Intrusion_detection_system
- Using PA-DSS certified solutions, pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php
- Firewalls, wikipedia.org/wiki/Firewall_%28computing%29
- PCI Glossary, pcisecuritystandards.org/security_standards/glossary.php
- White hat, wikipedia.org/wiki/White_hat_%28computer_security%29

Regulatory / Compliance
- EMVCo, www.emvco.com
- Health Information Privacy (HIPAA), www.hhs.gov/ocr/hipaa/