VISA PAYMENTS SECURITY TRAINING PROGRAM



GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

VISA Payments Security Training Program Training Course prepares payment professionals to protect card transactions across the full payment chain. It covers how card data moves from terminal to issuer, where it becomes vulnerable, and which controls reduce that exposure. Participants examine the Payment Card Industry Data Security Standard (PCI DSS), tokenisation, encryption, EMV chip technology, and 3-D Secure authentication in practical detail. Furthermore, the programme explains fraud typologies, chargeback management, and dispute resolution within card scheme rules. In addition, it addresses incident response, forensic investigation, and regulatory reporting. As a result, attendees can strengthen payment security with controls that meet scheme requirements.

VISA Payments Security Training Program Course Objectives

- Explain the card payment ecosystem and the roles of acquirer, issuer, processor, and merchant.
- Apply the Payment Card Industry Data Security Standard (PCI DSS) requirements to real environments.
- Implement tokenisation, point-to-point encryption, and key management controls.
- Explain EMV chip technology, contactless payments, and 3-D Secure authentication.
- Identify card-present and card-not-present fraud typologies and their indicators.
- Manage chargebacks and representments using card scheme dispute rules.
- Conduct risk assessments on payment channels and third-party service providers.
- Respond to data breaches using incident response and forensic investigation procedures.
- Apply the PCI Forensic Investigator process and card brand compliance reporting.
- Design layered fraud prevention controls using scoring, velocity checks, and machine learning.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Course Methodology

- Case studies on real card fraud schemes and breach incidents.
- Guided walkthroughs of PCI DSS requirements and compliance evidence.
- Hands-on exercises on fraud rule design and transaction scoring.
- Group work on chargeback case files and dispute responses.
- Tabletop simulation of a payment security incident and response.

Who Should Take This Course

- Payment security and fraud prevention specialists.
- Card operations and acquiring bank staff.
- Information security and compliance officers.
- Payment service providers and fintech risk teams.
- Internal auditors reviewing payment controls.
- Merchant risk and e-commerce operations managers.
- Consultants advising on PCI DSS compliance.

VISA Payments Security Training Program Course Outlines

Day 1: The Card Payment Ecosystem

- Participants in card payments: issuer, acquirer, processor, network, and merchant.
- Transaction flow from authorisation to clearing and settlement.
- Card data elements and the data storage prohibition rules.
- Merchant levels and validation requirements.

- Third-party service providers and their obligations.
- Payment channels: in-store, e-commerce, mobile, and contactless.
- Workshop: mapping card data flows across a payment environment.

Day 2: PCI DSS and Data Protection Controls

- PCI DSS structure: the twelve requirements and their intent.
- Scoping, segmentation, and reducing the cardholder data environment.
- Tokenisation and its role in reducing compliance scope.
- Point-to-point encryption and key management practices.
- Access control, logging, and monitoring requirements.
- Vulnerability management, secure development, and penetration testing.
- Exercise: preparing compliance evidence for an assessment.

Day 3: Authentication and Secure Technologies

- EMV chip technology and transaction cryptograms.
- Contactless payments and mobile wallet security.
- 3-D Secure authentication for card-not-present transactions.
- Strong Customer Authentication principles.
- Payment token standards and network tokenisation.
- Biometric and behavioural authentication methods.
- Workshop: reviewing authentication controls for an e-commerce channel.

Day 4: Fraud Detection, Chargebacks, and Disputes

- Card-present fraud: skimming, shimming, and counterfeit cards.
- Card-not-present fraud: account takeover and enumeration attacks.

- Fraud scoring, velocity checks, and machine learning models.
- Chargeback reason codes and the dispute lifecycle.
- Representment, pre-arbitration, and arbitration processes.
- Fraud reporting and scheme compliance programmes.
- Case exercise: building a fraud rule set and handling a chargeback file.

Day 5: Incident Response and Programme Governance

- Detecting and containing a payment data breach.
- Forensic investigation and the PCI Forensic Investigator process.
- Notification duties to card brands, acquirers, and regulators.
- Remediation planning and validation after a breach.
- Security awareness and internal training programmes.
- Metrics and reporting for payment security governance.
- Capstone: presenting a payment security improvement plan.

Conclusion

By successfully completing VISA Payments Security Training Program Training Course, participants will gain a practical command of payment security standards, fraud controls, and incident response. They will acquire the ability to apply PCI DSS requirements, design anti-fraud controls, manage chargebacks, and respond to breaches using recognised forensic procedures. As a result, they can reduce fraud losses and protect cardholder data across their payment channels. Gentex Training Center delivers this programme with a strong focus on real fraud cases and applied controls.

LEARN BOLD. **LEAD BEYOND**
GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

FAQs for the VISA Payments Security Training Program course

Q1 What is the "VISA Payments Security Training Program" course about?

It explains how card payments are secured end to end, covering the PCI DSS standard, tokenisation, encryption, EMV and 3-D Secure authentication, fraud detection, chargeback management, and breach response.

Q2 What are the key benefits of the "VISA Payments Security Training Program" course?

Participants reduce fraud losses, narrow compliance scope through tokenisation and segmentation, and handle chargebacks more effectively. They also respond faster and more correctly to breaches, which lowers scheme penalties and protects customer trust.

Q3 What skills will I gain from the "VISA Payments Security Training Program" course?

Applying PCI DSS requirements and preparing compliance evidence; implementing tokenisation, point-to-point encryption, and key management; detecting and preventing card-present and card-not-present fraud; and managing chargebacks, disputes, and payment security incident response.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "VISA Payments Security Training Program" course?

The course covers the Payment Card Industry Data Security Standard (PCI DSS), the PCI Forensic Investigator process, EMV chip technology, 3-D Secure authentication, Strong Customer Authentication, network tokenisation and payment token standards, point-to-point encryption and key management, penetration testing and vulnerability management, fraud scoring and velocity checks, chargeback reason codes, representment, pre-arbitration and arbitration processes, and card scheme compliance programmes.

Q5 How is the "VISA Payments Security Training Program" course applied in real-world practice?

Participants map card data flows across a payment environment, prepare compliance evidence for an assessment, review authentication controls for an e-commerce channel, build a fraud rule set, handle a chargeback file, and run a tabletop breach response. Each exercise mirrors daily work in payment security and fraud teams.