ONLINE TRAINING
Payments Security

CampusGuard's Payments Security Training Course equips security and compliance professionals with the knowledge and practical skills needed to protect payment ecosystems from end to end.

This course includes the following modules:

- **Revenue Approval:** This module provides an overview of how revenue activities are approved, managed, and monitored. Staff will learn why formal approval is required before accepting payments, what offices are typically involved, and how consistent processes protect the institution, employees, and customers from fraud.
- **Cash Handling:** This training module provides faculty, staff, and student employees with the knowledge and awareness required to securely handle cash and cash-equivalent transactions. It covers risk awareness, organizational requirements, security practices, documentation standards, and reconciliation procedures.
- **Check Handling:** This module provides an overview of proper check handling practices from the moment a check is received, through storage, deposit, and reconciliation. Learners will review common check fraud risks and red flags and apply physical security and segregation of duties requirements, as well as learn when and how to report issues or suspected fraud.
- **Payment Fraud Examples in Higher Education:** Due to the complex environments within higher education, with decentralized departments, student trust, and high transaction volumes, colleges and universities often experience payment fraud. This module provides an overview of common payment fraud examples within higher education and how to identify red flags.
- **Common Payment Fraud Scenarios Review:** As a follow-up to the previous module, learners will step through real-world scenarios and learn to identify red flags and recommended courses of action.

Payments Security

- **Electronic Payments:** Electronic payments are transactions completed without physical cash or checks, typically through digital systems. This training module reviews common electronic payment types, evolving trends, and increasing risks.

- **Evolving Payment Technologies:** Consumers and students increasingly expect quick, convenient, and secure ways to pay for tuition, housing, campus services, and online purchases. Evolving payment technologies, like digital wallets and contactless payments, offer quick payment options, but don't come without risk. This training module helps staff understand these evolving payment technologies and related risks.

- **Bank Secrecy Act/Anti-Money Laundering:** While colleges and universities are not banks, they frequently process financial transactions that can be targeted for money laundering, fraud, or misuse of funds. This module builds awareness of Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) concepts, focusing on what staff should recognize, document, and escalate.

Key Takeaways:

This course equips teams to:

- Follow institutional approval and payment processes to protect the institution, staff, and customers
- Apply secure cash and check-handling practices from receipt through reconciliation
- Identify payment risks and fraud across cash, checks, electronic payments, and refunds
- Use internal controls to prevent fraud and errors
- Manage risks associated with electronic and emerging payment technologies

Target Audience: Staff and students who are responsible for incoming and outgoing payments for events, fees, merchandise, or services. Business officers, reconciliation, refund management, accounts payable, or any staff who manage the movement of money.

Course Length: Each micro-module is 8-12 minutes long; total time: approximately 90 mins.

DEMO

Want to see more? Request a free demo!