SECURUS Technologies™

GOVPAYNET®
The Simple Way To Pay

Mitigating Security Risks Associated with Credit Card Payments

Mitigating Security Risks - Overview

What Are The Risks?

Risks to be managed include:

- Employee theft
- Payment portal – PCI compliant?
- Handling and safeguarding of credit card data
- Information storage security and potential POS attacks
- Transaction data transmission and encryption
- Network security

Dos and don'ts of credit card payments

Small Group Breakouts

Small group discussion of the dos and don'ts of accepting credit card payments

Compliant environment - the dos

A compliant process or procedure that mitigates the risk of fraud.

War stories – the don'ts

Most of us have either heard about or actually experienced a situation where something went awry.

Dos and don'ts of credit card payments

Small Group Breakouts (cont'd)

Dos and don'ts – report back and share with larger group

GovPayNet War stories
- Anecdotes from correctional facilities and county jails

Risk Assessment

Self-assessment

- Each agency to complete an assessment and calculate their score

- Validation of current safeguards and compliance processes

- Potential items to address or evaluate further

    - 'The bad news is the good news if you know what to do with it'

Mitigating Security Risks

How To Mitigate The Risks

- Employee training on how to identify and mitigate fraudulent activities
- Restrict access of data to need-to-know only
- Automatic intrusion detection and prevention solutions
- Antivirus protection – Continuous update of the software
- Data encryption – Of the data in use, in transit and at rest
- Secure storage of data and backups of data
    - Never store payment card information or pin numbers
- Assign unique ID to each person with computer access
- Protect the POS devices from modification or manipulation

Mitigating Security Risks

Example of successful deployment

Securus Technologies

*PCI Merchant Level 1 Compliant

        - For merchants with more than 6 million Visa or MC transactions annually

Steps taken:

- Limited physical access to the compliance environment
- Limited physical access to the data center
- Associates trained on how to accept payment cards
- Associates trained on requirements while in the environment
- Setup IDS and IPS for the environment
- Segregated the Compliance environment from the Corporate environment
- Third party audit of the environment to get the ROC (Report on Compliance)
- Associates are not allowed to record any Payment card data external to the system

Recent Changes and Future Trends

What does now and the future look like?

EMV – chip technology, fraud reduction, phased deadlines

Tokenization – the safe way to 'store' data

Mobile payments – Using smart phones in place of credit cards

Better collaboration between financial institutions – Being able to make payments from one financial institution to another seamlessly and securely

Phone to phone payment transfers – Currently requiring a financial institution between but eventually able to transfer funds without a middleman

Better Security with out impacting the customer experience – More use of technology to improve security, taking the user out of the equation

Back end innovation – Moving from older traditional financial transactions after the purchase to immediate and electronic transactions

Advantages of accepting credit cards

Why Do It?

- Convenience – taxpayer friendly, another option…
- Improves agency's cash flow
- Efficiency
- Reduces costs, time and risks of processing checks
- Online payment option reduces traffic at counter
- Immediate authorization, unlike checks that can be returned

Lessons learned

What are the potential pitfalls?

Potential costs, sometimes hidden

- Set-up, equipment
- Access, monthly and/or miscellaneous fees

Software company can 'hold you hostage'

Chargebacks – aka "adjustments"

Contract terms can be restrictive in some cases

Technology issues

Recap

Key Take-aways

- Know the risks, and take steps to mitigate them
- Follow best practices (dos) and avoid worst practices (don'ts)
- Self-assessment – key action item or two for your agency?
- Try to stay current on technology changes and trends
- If you don't accept credit cards currently, should you?
- If you do accept credit cards, try to avoid the pitfalls

Thank You for Your Participation !