W3C Web Payments
E-commerce Security Task Force

DRAFT - Work-in-Progress

Executive Summary & Agenda

Executive Summary: The purpose of this presentation is to provide a point of view on the critical importance of e-commerce security and establish the foundational focus of a task force to perform a security evaluation of the web payment specifications with the intent of promulgating best practice guidelines for eco system participants.

Proposed Agenda

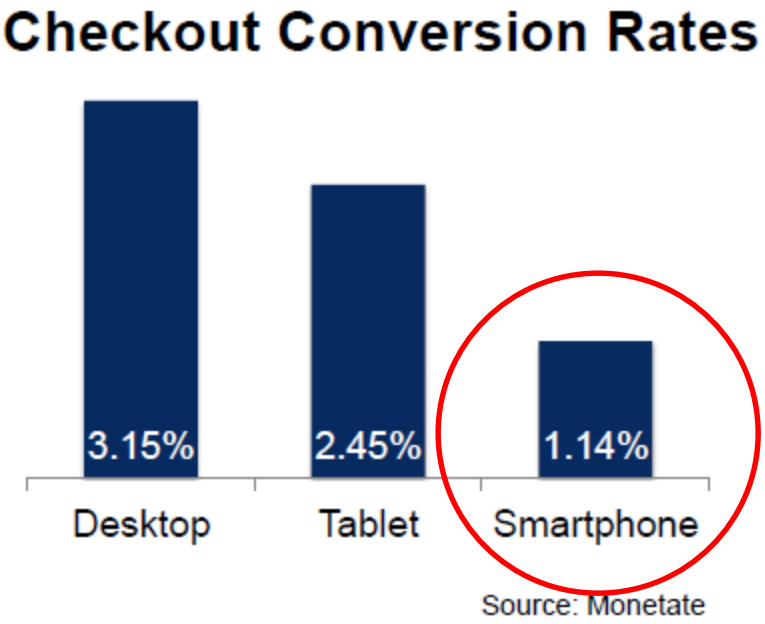
- Mobile is the Challenge
- Balancing Security with the UX
- E-commerce Security Policy Environment
- Typical E-commerce Security Considerations
- Security Threats
- Security Vulnerabilities
- Available Security Tools
- Next Steps
- Appendix

E-commerce Pain Point – Mobile's the Merchant's Biggest Challenge

Checkout Conversion Rates by Device

Mobile Device Challenges

- Slower load times
- Smaller screens
- Tiny keyboards



Source: Glenbrook AXP Seminar – Digital Checkout April 21, 2016

E-commerce Security –What's the Challenge?

Google's View of the Shopping challenge - *Why users abandon mobile* ***purchase forms:***

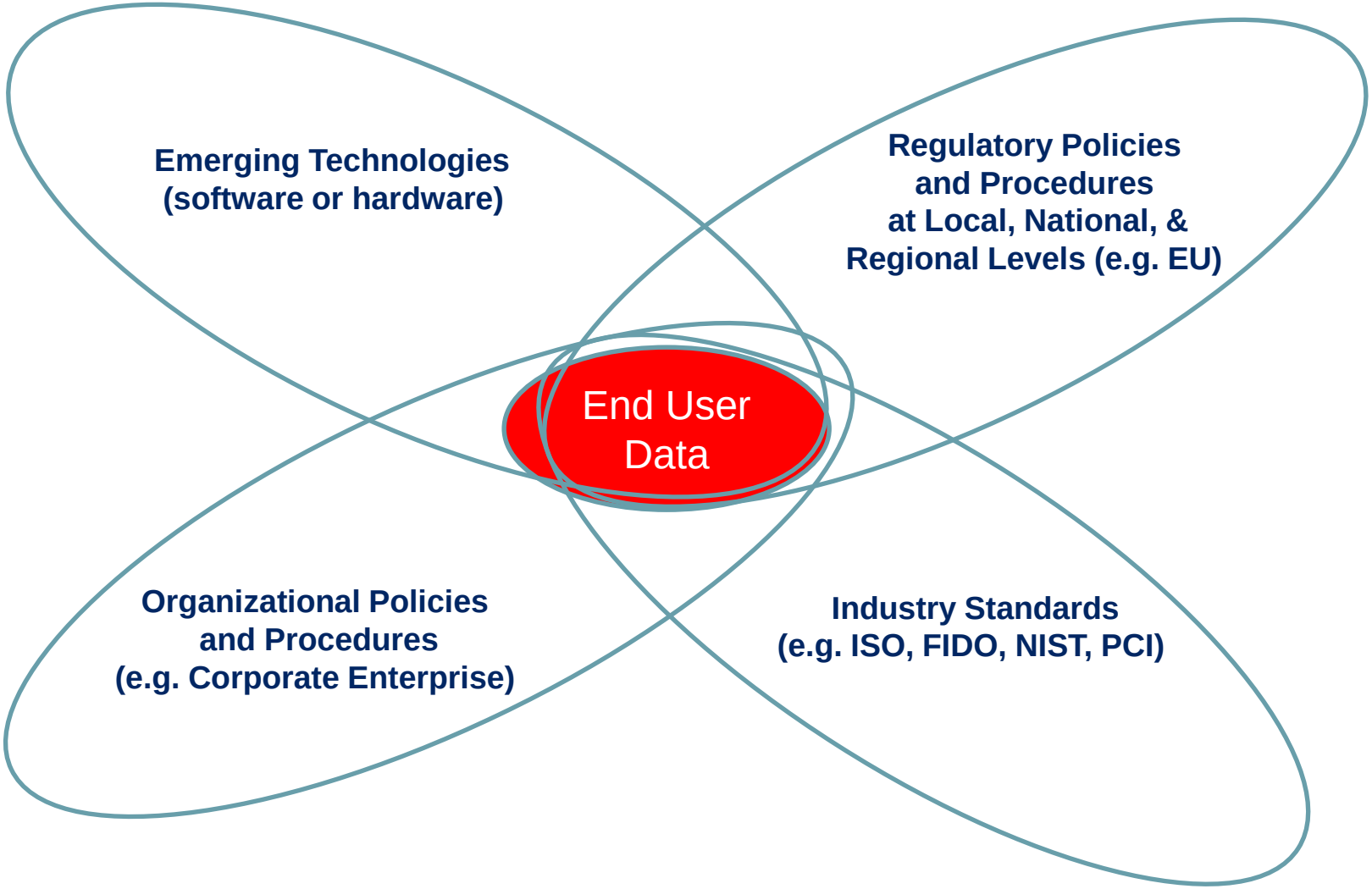
User-intensive	Difficult to use	Slow to load and refresh	Require multiple steps to complete

"This is because of two primary components of online payments— security and convenience—often work at cross-purposes; more of one typically means less of the other."

Source: https://developers.google.com/web/fundamentals/discovery-and-monetization/payment-request/

Payment Request API: An Integration Guide

E-commerce Security Policy Environment



Typical Elements of E-commerce Security

User Privacy and Protection – The action to defend and keep safe sensitive and private data, communications, and preferences.

Authentication - the process or action of verifying the identity of a user or process.

Authorization - the action or fact of giving permission or approval.

Nonrepudiation - The assurance that someone cannot deny something.

Confidentiality - a set of rules that limits access or restricts certain types of information.

Integrity – An unimpaired or uncorrupted condition.

Service Availability - Ability of an IT Service to perform its agreed function when required determined by Reliability, Maintainability, Serviceability, Performance and Security.

Common E-commerce Security Threats

Key Vulnerabilities

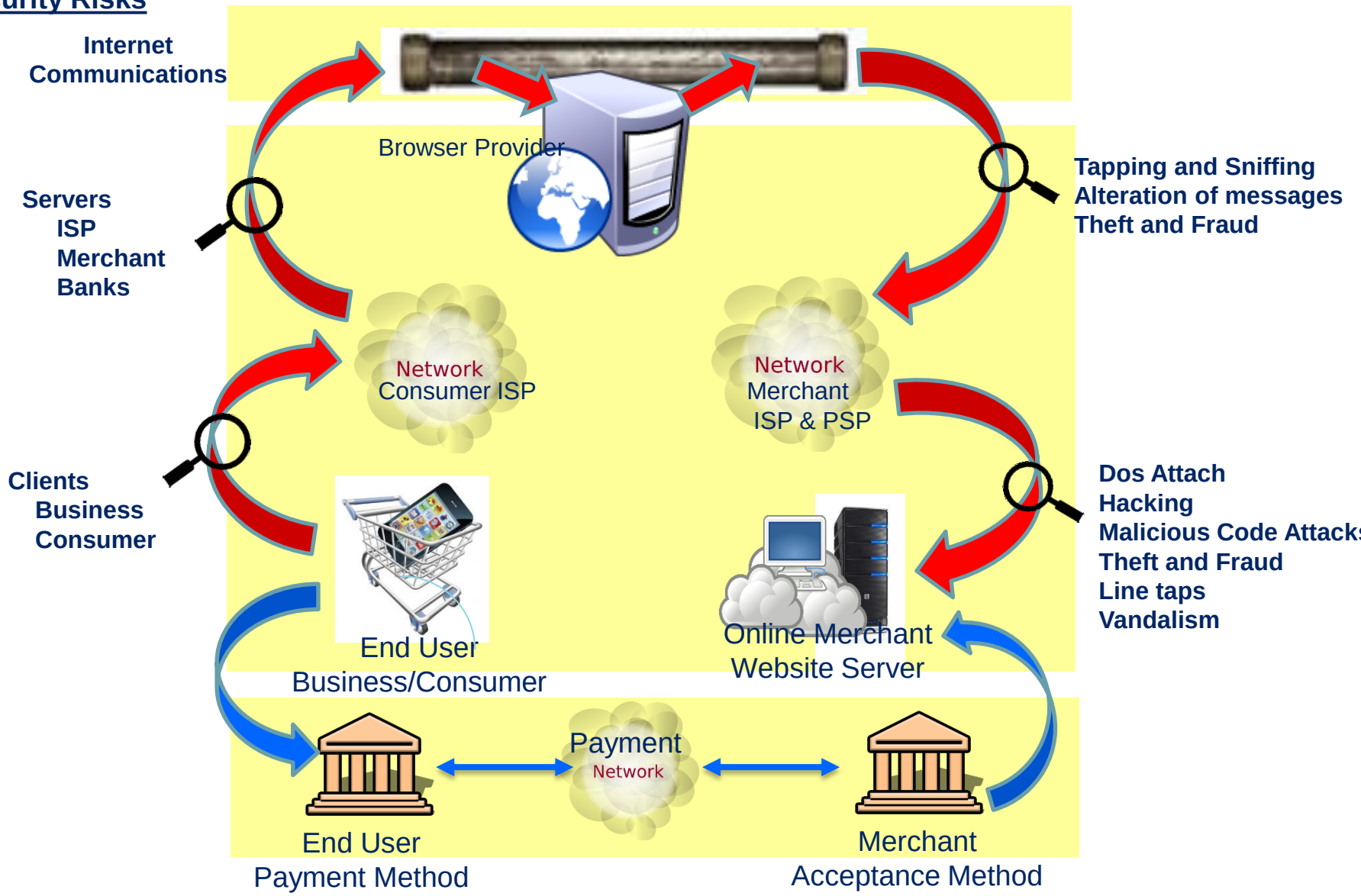
- Client
- Server
- Communications

Most Common Threats

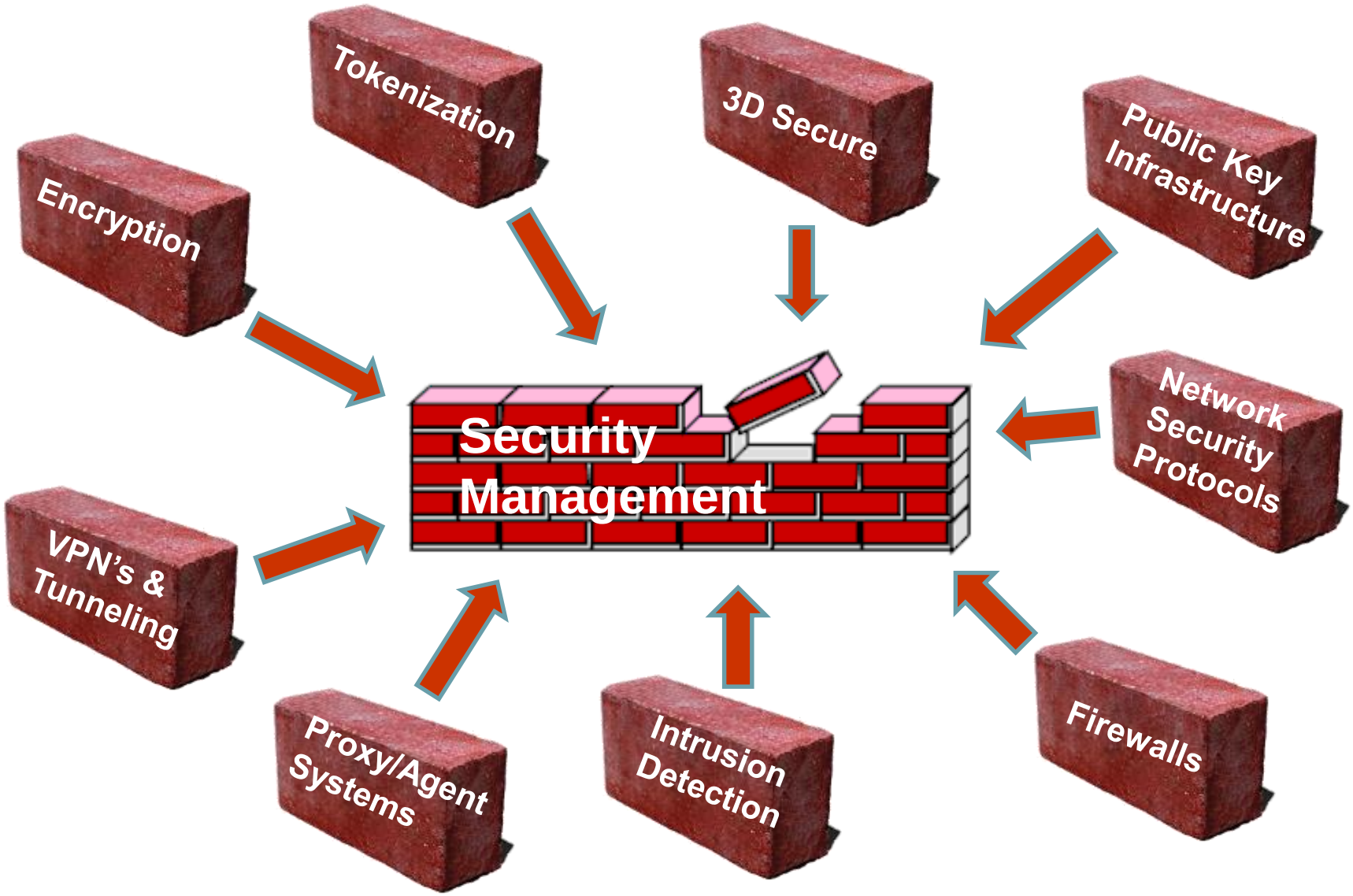
- Malicious Code
- Hacking and cyber-vandalism
- Credit Card Fraud/Theft
- Spoofing
- Denial of service attacks
- Sniffing
- Insider Jobs

E-commerce Environment Security Vulnerabilities – Layman's View

Security Risks



E-commerce Environment: Available Security Tools



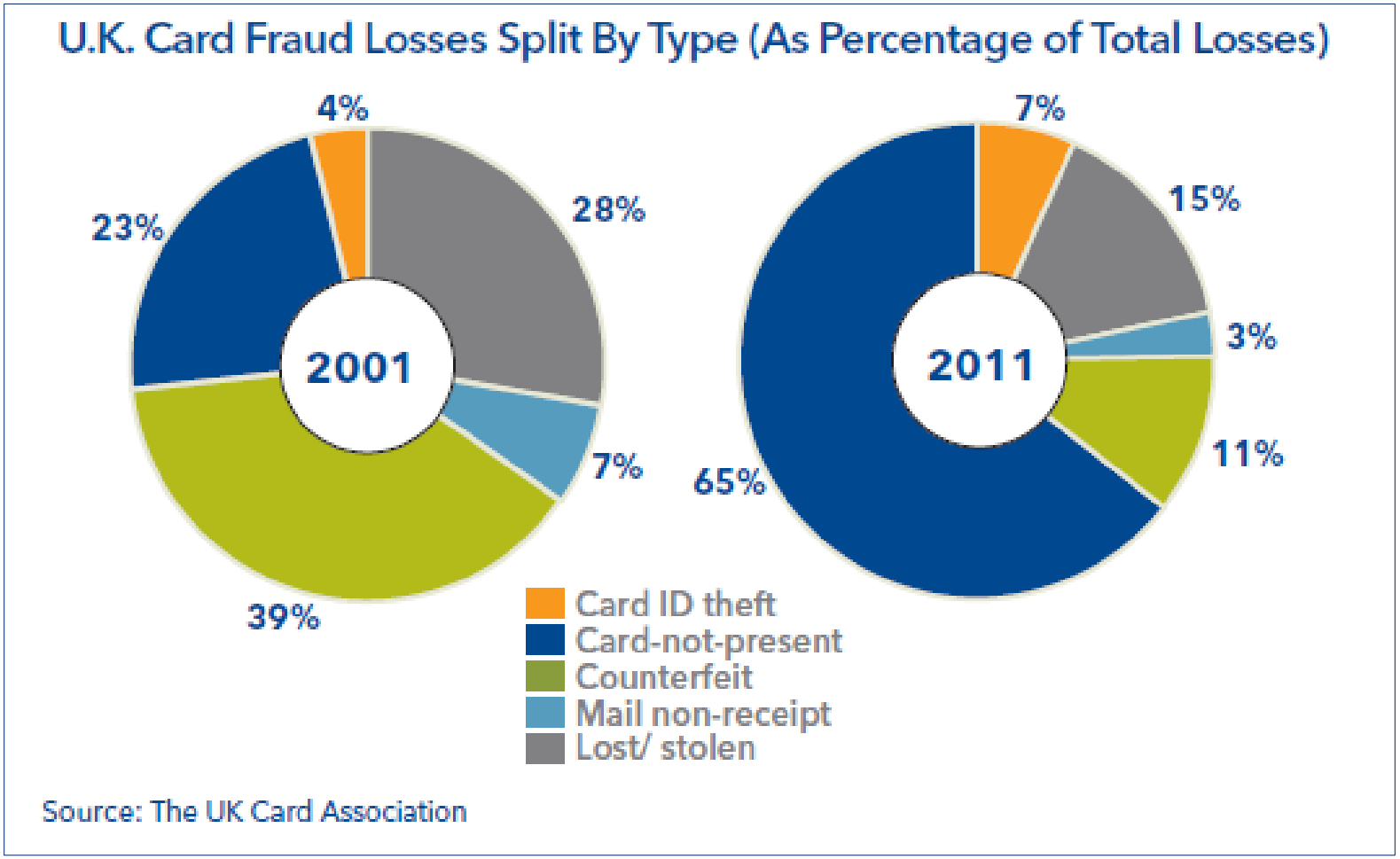
W3C E-commerce Security TF – Next Steps

- Assign an e-commerce Security Task Force Project Leader / PMO
- Recruit the right talent from Membership
- Align with other security/payment industry focused groups (PCI, X9, FIDO, EMVCo)
- Conduct a security analysis of the specification to uncover vulnerabilities
- Perform an security evaluation of the identified vulnerabilities to promote mitigation and remediation options.
- Aggregate options and determine best practices.
- Publish Security Evaluation and Best Practices as Notes

APPENDIX

E-commerce Security : US EMV Migration Fraud Implications

Lessons Learned from the U.K. EMV Deployment



12

E-commerce Security: The Impact of Security on Consumer Online Shopping

2016 AmEx Digital Payments Security Survey

- 70% of U.S. merchants are experiencing an increase in sales through online and mobile channels over the previous year
- Nearly half (48%) of consumers who shopped online in the past year have experienced payment fraud, representing nearly 80 million online consumers.
- Meanwhile, 60% of merchants report that they have experienced fraudulent online sales.
- 25% say their level of fraud with online sales has increased this year. They are investing 28% of their IT budgets on payment data security