PCI Security Standards Council

North America

# Community Meeting 2023

PCI Security Standards Council

# How to Protect Your Ecommerce Transactions

An Overview of PCI DSS v4.0 Changes for Ecommerce Sites (SAQ A, A-EP, D, ROC)

securityMETRICS®

# Gary Glover

VP of Assessments

- 18 years in Cybersecurity and Payment Card Industry
  - Participate in SIG's, GEAR, etc.
- 10 years as a Software Developer
- 7 years as a Mechanical Engineer

PCI Security Standards Council

# Changes in eCommerce Threats

Most Common Threats Based on Forensic Analysis

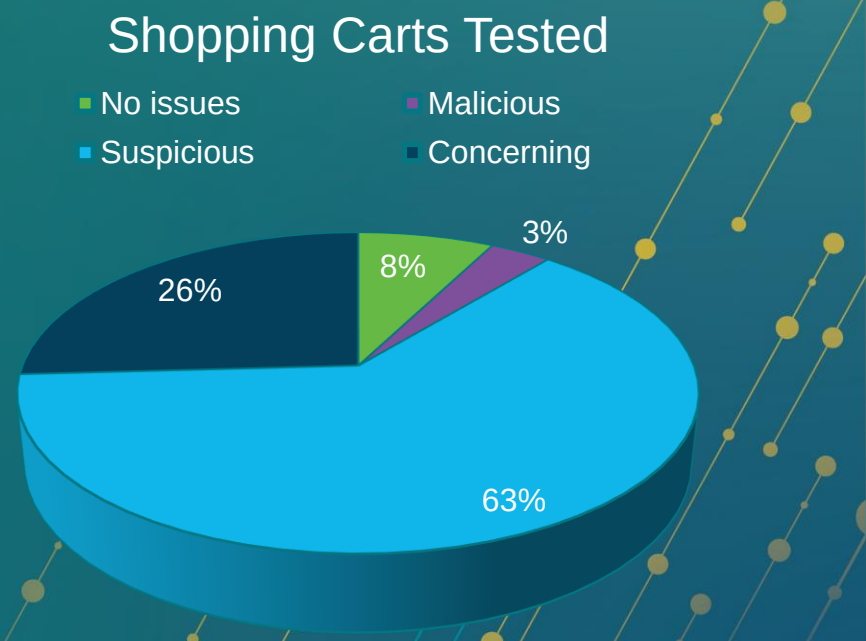
- What attacks are most common lately?
  - eCommerce skimming
  - iFrame integrity compromises
    - Source change
    - Redrawing
  - Malicious scripts included
- Skimming not visible to customer or processor

PCI Security Standards Council

# eCommerce Threats Today

eCommerce Primary Research being Conducted by SecurityMetrics

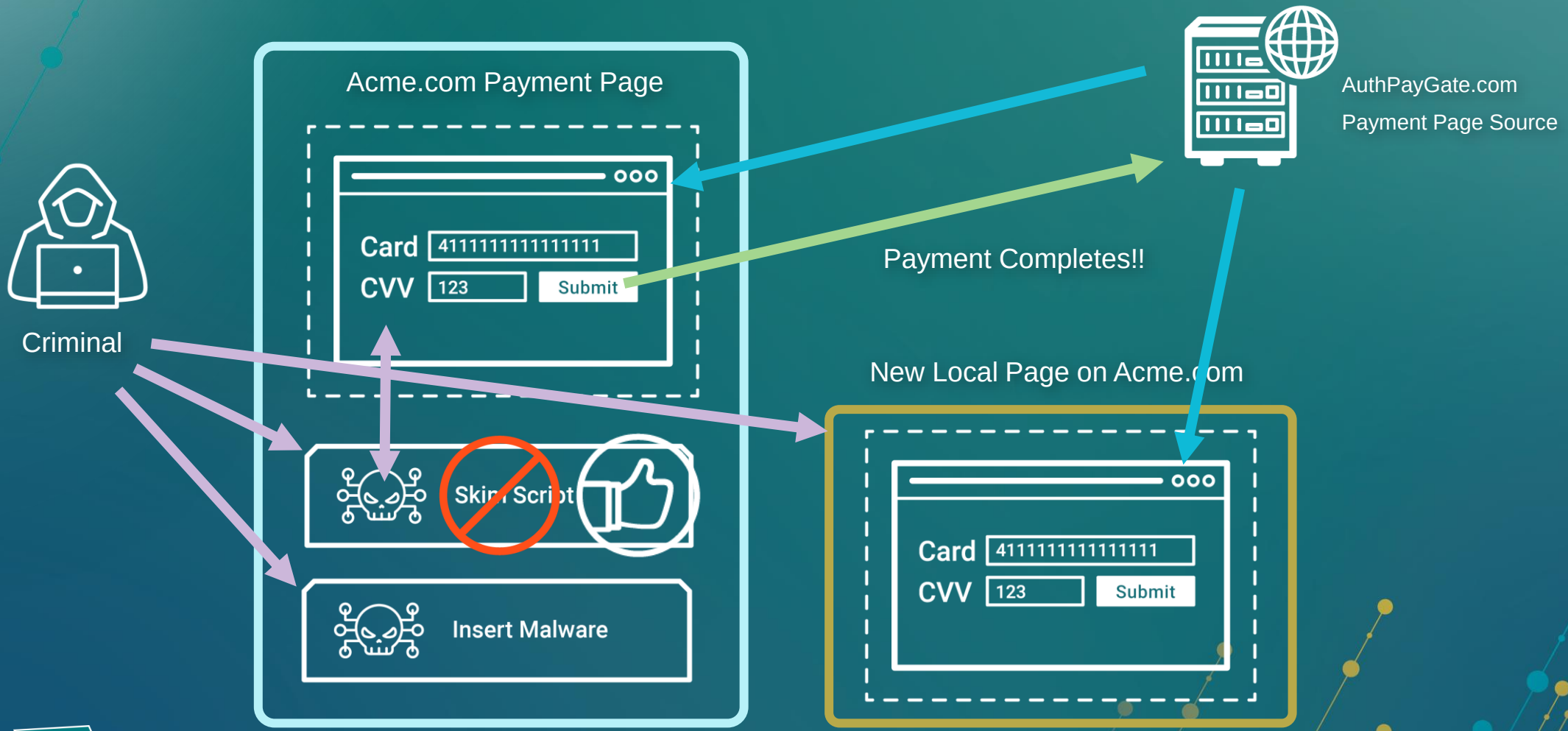
- Internet eCommerce Research
  - 52 million eComm sites worldwide
  - Risk Check tests for common vulnerabilities, no false positives
  - Results
    - 29.7% of these sites had serious vulnerabilities
    - Only 17% were using CSP or SRI
- Shopping Cart forensic investigations
  - 1400 sites reviewed for skimming attacks
  - 92.4% of sites had security issues
  - 2.44 issues per site on average




PCI Security Standards Council

# Demo of an iFrame Skimming Attack

iFrame Same Origin Policy Defeat




PCI Security Standards Council

# How Fight Skimming Attacks?

- Most malicious scripts are very difficult to find
  - Analysis and scanning must occur in the browser execution environment (Document Object Model - DOM)
- PCI DSS v4.0 adds requirements to help
  - Dynamic script scanning really is needed
- What should eCommerce Merchants do?
  - Goal is to regain control of referring pages and payment pages
  - Start now testing tools

# PCI DSS 4.0 Addresses Threats

Requirements 6.4.3 and 11.6.1 Added to Control Trends in eCommerce skimming

- Requirement 6.4.3 – keep track of scripts used
  - We have found over 300 scripts on a single payment page
- Requirement 11.6.1
  - Periodic (weekly) scanning to detect changes or additions
  - Consider use of prevention HTTP techniques (SRI, CSP)
  - Hard to search pages generated dynamically
- End Result: controlled, simpler, & secure payment pages

PCI Security Standards Council

# SAQ A eCommerce Requirements

- Changes to SAQ A will be a challenge
  - ASV scanning
  - Future dated script scanning
- How to get ready?
  - Start ASAP getting used to doing ASV scans
  - Start testing tools for script scanning requirements
- There won’t be a delay in PCI DSS v4.0 deadlines
  - If using iFrame redirect - investigate script tools

PCI Security Standards Council

# Script Scanning Tools

What are characteristics of these tools?  What is needed?

- Detect changes/additions on payment pages via DOM
- Tool setup types
  - Agentless
  - Agent installation required by merchant
- Not like VA scan, much more complex
- Ease of use for merchants is important for adoption
  - SAQ A, A-EP, & D
- Start testing soon so you are ready for March 31, 2025

# Key Takeaways

- New eCommerce attacks are real and prevalent
- Changes to PCI DSS v4.0 help address threats
- Work with SAQ A merchants as early as possible
- Join Risk Check research

PCI Security Standards Council

PCI Security Standards Council

# Thank You!