



# “Commercially Reasonable” Security

## Measuring Up to the New Standard

Presented By:  
Tom Hinkel, Director of Compliance  
Safe Systems, Inc.

# Agenda

- Definition of Commercially Reasonable Security (CRS)
- Building a case for CRS
- Regulatory guidance, best practices, and industry standards
- What's the answer?
- Summary
- Q&A

# Definition of CRS

- *Commercially reasonable* effort is a term **incapable of a precise definition** and will vary depending on the context in which it is used. It is based upon a standard of reasonableness, which is a **subjective** test of what a reasonable person/business would do in the individual circumstance, taking all factors into account. – *USLegal.com*
- An important factor in determining the security methods that are “commercial reasonable method” is the security method in use by “similarly situated banks for similarly situated customers”. - UCC-4A

# Definition of CRS

- FFIEC:
- Practices and procedures in widespread use in the business community generally considered to represent prudent and reasonable business methods.
- “Whether a method is a commercially reasonable system depends on an evaluation of the circumstances.”
- “What constitutes a commercially reasonable system may change over time as technology and standards evolve.”

# Why is CRS Important?

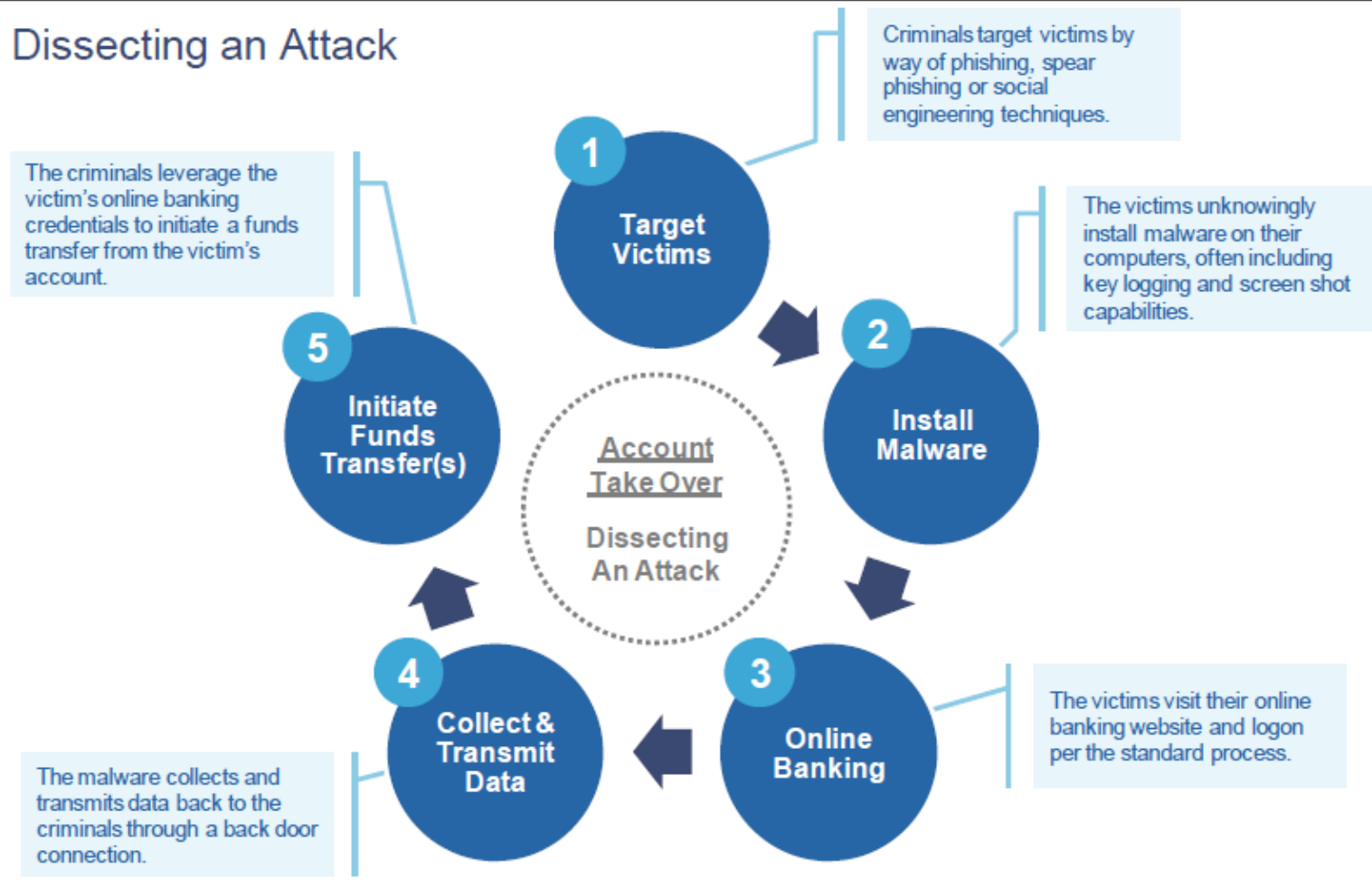
- Liability for unauthorized transfers from consumer accounts is addressed by Regulation E.
- Compliance with the FFIEC Guidance does not necessarily insulate a financial institution against potential liability for losses caused by unauthorized payment orders or fund transfers that are charged against a commercial customer's account. That question is governed by and hinges upon the loss allocation rules of Article 4A of the UCC.
- Under UCC Section 4A-202: "...a payment order is effective as the order of the customer, whether or not authorized, if the security procedure is a commercially reasonable method of providing security against unauthorized payment orders."

# Why is CRS Important?

- Shames-Yeakel vs. Citizens Financial:
  - *The judge determined **commercial reasonableness** by indicating that there are technologies and tools available in the marketplace today, albeit not in wide use in banking, which the bank could have employed to assist the company.*
- Experi-Metal, Inc. vs. Comerica Bank:
  - *The court concluded as a matter of law that the defendant bank's use of token-technology constituted "**commercially reasonable** security procedures." Now awaiting verdict.*
- Patco Construction Company, Inc. v. Peoples United Bank d/b/a Ocean Bank:
  - *Claim is that the Bank failed to provide **commercially reasonable** security procedures that would permit the Bank to shift liability for unauthorized payment orders to Patco.*
- Choice Escrow and Land Title, LLC vs. BancorpSouth Bank
  - *...security procedures and/or authentication methods used by BancorpSouth (both Single Control and Dual Control) were not **commercially reasonable** methods for providing security against unauthorized payment orders.*

# Typical Business Account Takeover

## Dissecting an Attack



**Figure 2: Dissecting An Account Take Over Attack**

# New FFIEC Guidelines

- Supervisory Expectations
  - Risk Assessments – Periodic (at least every 12 months), not just initial
    - Existing threats
    - Changes in the customer base
    - Changes in functionality
    - Actual incidents
    - Changes in the threat environment

# New FFIEC Guidelines

- Supervisory Expectations
  - Customer Authentication for “High Risk” transactions
    - Consumer – lower risk, but consider MFA
    - Commercial – high risk, must offer MFA
  - Layered Security
    - Prevent (missing in draft, but required)
    - Detect and Respond
    - Control of administrative functions

# New FFIEC Guidelines

- Supervisory Expectations
  - Customer Awareness and Education
    - An explanation of protections provided and not provided under Reg. E
    - How and why the institution may contact customer regarding their credentials
    - Suggestion that customer periodically perform RA and control evaluation
    - List of possible risk controls customer might implement
    - List of institution contacts for reporting suspicious activity

# What's the Answer? Best Practices

- Prevent
  - MFA
    - Something you know
    - Something you have
    - Something you are
  - Out of Band Authentication/Confirmation
    - Fax
    - Phone Call
    - SMS (Text Message)
  - AV/Anti-Malware Software
  - Customer Selection & Risk Classification
  - Customer Education
  - Pre-authorized Recipient Lists

# What's the Answer? Best Practices

- Detect
  - Metrics & Monitoring
    - Amount & Frequency (pre-set)
    - Time of Day & Day of Week
    - Anomaly (deviation from established patterns)
    - Device Identification
      - One-time cookies
      - IP address
      - Geo-location
    - Challenge Questions

# What's the Answer?

## Best Practices

- Respond/React
  - Coordinate with incident response program
    - NPI involved?
  - Re-evaluate customer risk
  - Enforce provisions of contract
  - Vendor support expectations?
  - Forensics
    - Isolate PC
    - Chronology of events
  - Report – SAR, FBI, police

# Beyond CRS

- “Establishing commercially reasonable security procedures (or agreeing to them) will not necessarily be the end of the story for the bank. Of apparently equal importance are the activities undertaken by the financial institution in reacting to possible fraud.”

- *Pierce Atwood, LLP*

# Summary

- Implement risk based-processes and controls that are consistent with those of other financial institutions of a similar size and complexity.
- Periodically evaluate and modify security strategies based on new guidance, industry standards, best practices, and **changes in the internal and external threat environment.**

# Questions?



[www.FFIECguru.com](http://www.FFIECguru.com)  
[www.safesystems.com](http://www.safesystems.com)

Tom Hinkel, CISA, CRISC - Director  
of Compliance, Safe Systems, Inc.  
[tom@safesystems.com](mailto:tom@safesystems.com)