Digital Authentication for an Analog World

Robert W Capps II

Chief Technologist

World Savings Bank, FSB

The views expressed in this presentation are mine; they do not necessarily reflect those of my employer, World Savings Bank, FSB or its parent company, Golden West Financial.

No one wants to hear me talk for 20 minutes

I’m not going to read my paper

I love questions

This presentation is assumed to be from the viewpoint of a financial institution.

Key Concepts

Current online authentication techniques are weak at best:

- Most rely on multiple single factors
- Credentials are easily stolen from consumers and rarely change
- Lack of consistency in authentication processes confuse consumers
- They do not build upon or mirror current offline processes

Key Concepts

Who’s At Fault:

- No individual contributor is at fault
- This is really a failure of multiple parties
  - OS Providers
  - Browser Providers
  - Financial & Commerce Software Providers
  - Security Vendors
  - The Financial and Commerce Institutions

Key Concepts

Authentication Security Begins With:

- The OS
- The Internet Access Software
- The ISP
- The Financial & Commerce Software (Web, Back-end)
- Financial & Commerce Institution Security Processes

Key Concepts

The OS

- Must have security/auth services baked-in
- Must not rely on 3rd party applications to enforce security/auth processes
- Best position within the consumer access stack to enforce consistency

Key Concepts

The Internet Access Software

- Must contain consistent security/auth processes and indicators for consumers
- Must not try and re-invent the security wheel

Key Concepts

The Financial Services Software Vendors

- Must interface with browser and OS auth processes
- Best position to enable rich meta data review and transaction scoring
- Could enable data sharing for fraud detection

Key Concepts

Financial and Commerce Security Processes

- Must tie together transactional fraud monitoring with consumer web access monitoring
- Must aggregate and share fraud data between institutions
- No more signature processes

Key Concepts

The Holy Grail - Strong Authentication:

- Customer auth credentials must be usable in multiple channels
- Authenticators cannot be passed between humans for authentication
- Must scale well -
(avoid token necklace or fat wallet syndrome)
- Scale auth technique to transaction risk
(profile transactions and respond as needed)

Key Concepts

FFIEC Guidance as First Step

- Does not go far enough...
- No oversight for Commerce Institutions
- Does not require institutions to standardize auth processes and techniques
- Most current consumer visible solutions are not yet ready for prime-time
- If this migration is not designed and managed well, consumers may reject changes

Key Concepts

Steps 2-10 - We Must Partner

- Standardize . . . Process
- Standardize . . . Consumer Visible Indicators
- Standardize . . . Credentials

Key Concepts

Conclusion(s)

We must form a long-term partnership to ensure that the critical online channel is not lost to fraud and other criminal operations

Innovation and standardization will present mitigating alternatives to online (and offline) risks

We cannot afford to focus on securing only one channel . . . fraud will move to the path of least resistance

Questions?

Thank You!