Improving Customer Authentication

Presented to the

Retail Payments Risk Forum
A CATALYST FOR COLLABORATION

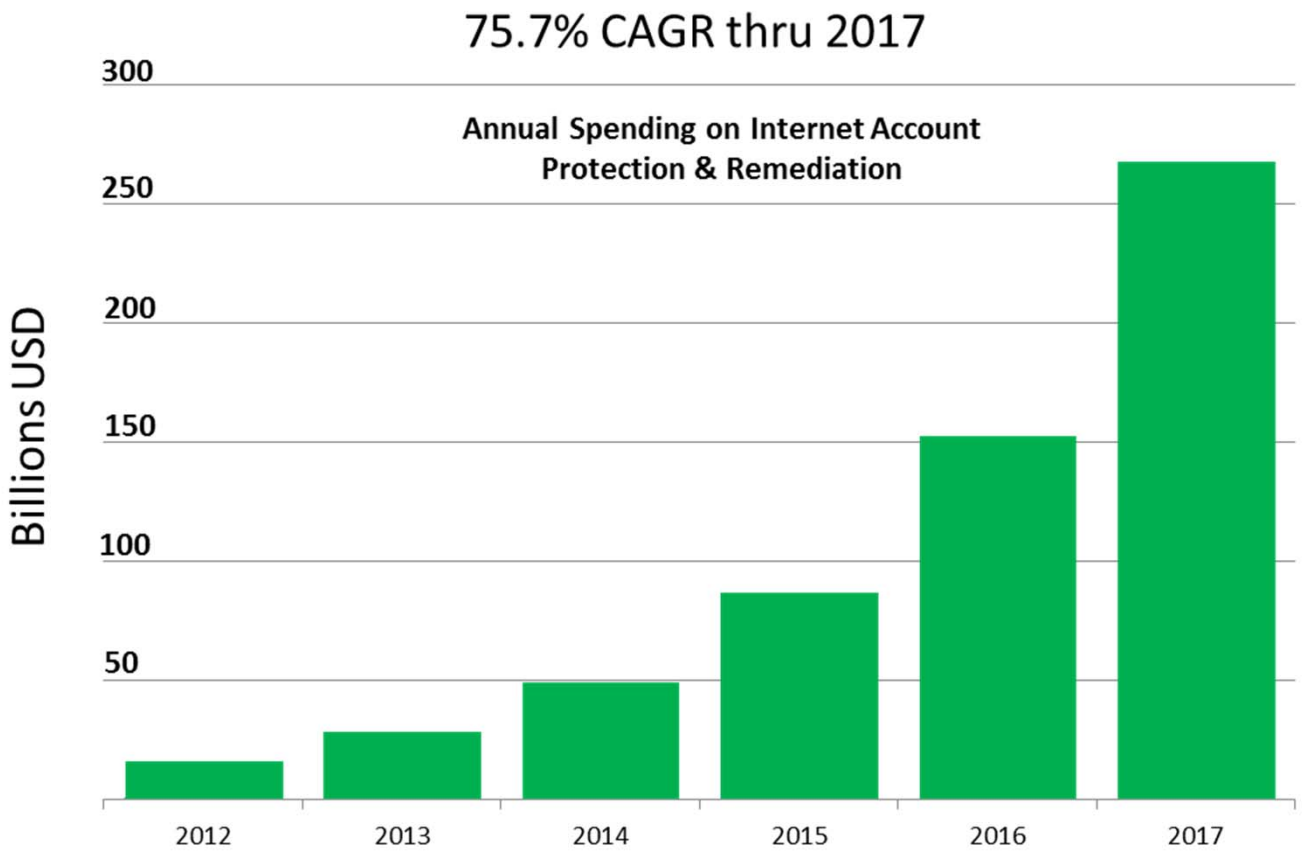
July 31, 2013

FEDERAL RESERVE BANK of ATLANTA

Authentify, Inc.
Peter Tapling
peter.tapling (at) authentify.com
+1-773-243-0322

Happy 20th Birthday!

An Expensive Problem



Sources: United Nations Comprehensive Study of Cybercrime, February 2013
U.K. Ministry of Defense, Measuring the Cost of Cybercrime, R. Anderson et al.

What do these have in common?

Setting the Bar

Who are you?

- Identity
  - You are the person your mother knows you to be
- Who does society know you to be?
  - Societal identity is developed over time
    - Starts with birth certificate; citizenship
    - Academic/health records
    - Employment records
    - Legal records (land ownership, driver's license)
    - Financial records
- We all have "personas"
  - Employee, taxpayer, consumer, guardian, business owner

Proving Whom You Are

- **Authentication:**
  - "The verification of the identity of a person or process."

    The Free On-line Dictionary of Computing
    ©1993-2001 Denis Howe
  - Is the party presenting themselves now the *person* whom we believe owns the identity being claimed?

- **Authorization:**
  - "Permission or power granted by an authority."

    Dictionary.com
    ©2013 Dictionary.com, LLC
  - Are you allowed to do what you are asking?

Authentication Building Blocks

- Accepted authentication factors:
  - Something you know
  - Something you have
  - Something you are
- Layering is good, but multiple “somethings you know” is not multi-factor
- Many other elements figure into *risk*
  - Where are you? What other charges have occurred? Time of day? Card from compromised batch?

Many Options

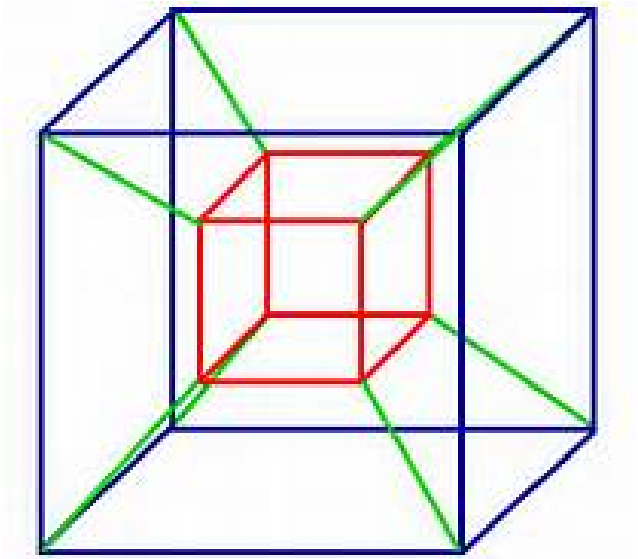
- Somethings you know
  - Passwords; PINs; images; KBA
- Somethings you have
  - Card; tokens; phone
- Somethings you are
  - Finger; voice; facial; gesture; keystroke

- Hundreds of “authentication” vendors

- Today, all basically supplement a user name/password

Multi-Dimensional Challenge

- The 4 dimensions of the Authentication Tesseract:
  - Factors
  - Sources
  - Communication channels
  - Data acquisition channels



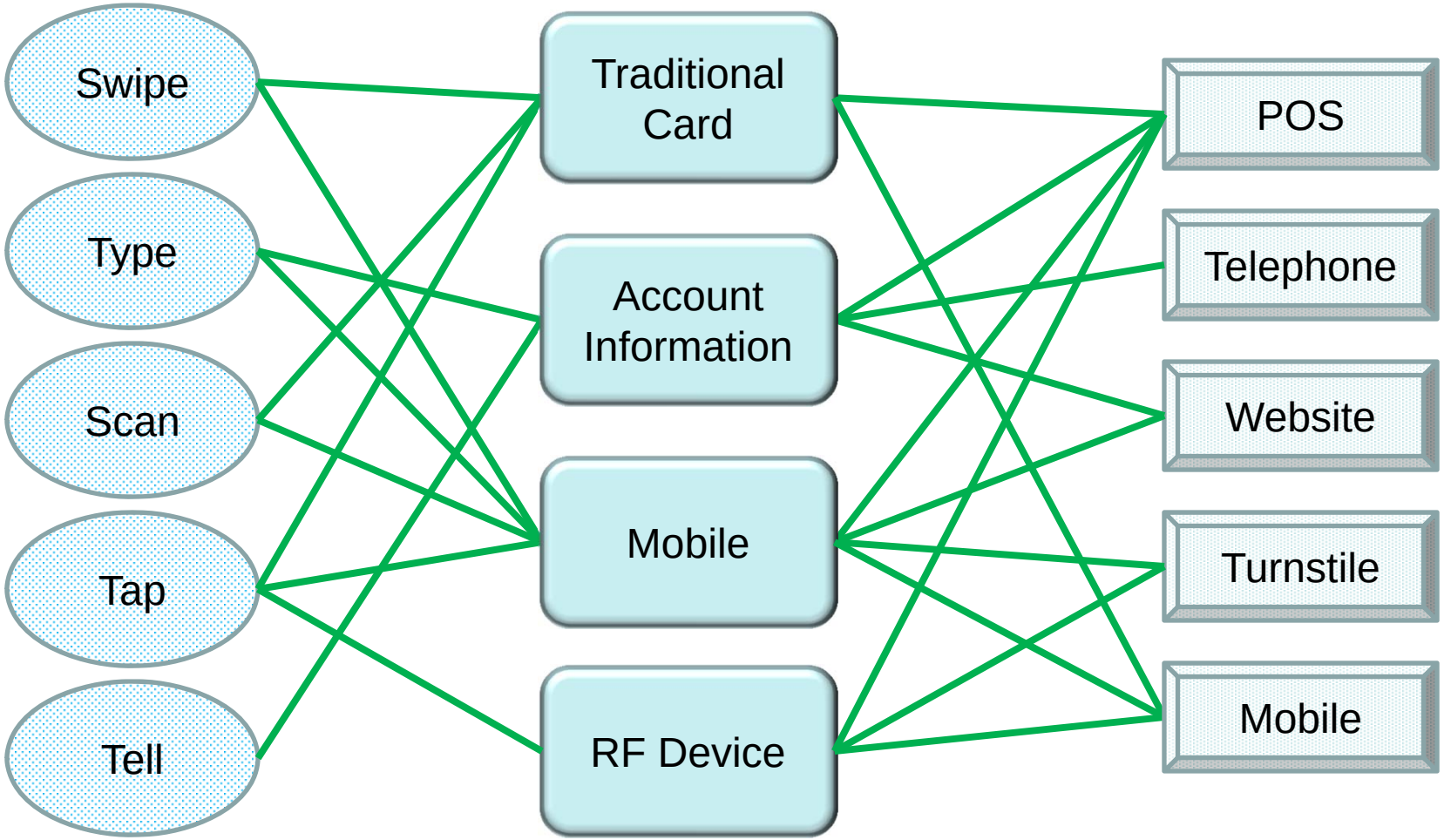
- Analyze your risks and fraud vectors
  - What can go wrong and how?
  - How can risks be mitigated in each dimension?

Why Are Attacks Prevalent Now?

- Once expensive computing resources now cheap
- Multitude of applications for variety of purposes
- Bad guys like to “work from home”
- Automation of attacks creates value in any breach
- As consumer demand pushes us to mobile, we are trying to “stretch” existing infrastructure
- End points under consumer control

- BUT – end user convenience remains critical to success!

How Do People Pay?



What Are Payments?

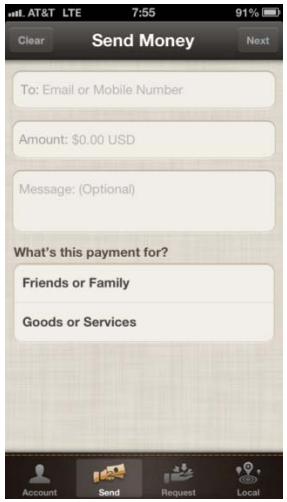
- With regard to mobile, they must be electronic
  - ACH; wire; credit; debit; [check (EPO)?]
  - These are the payment rails today; other schemes generally jump on board
  - Even “closed” systems eventually settle over these networks
- They all operate under different rules
  - Are there different considerations for “mobile”?

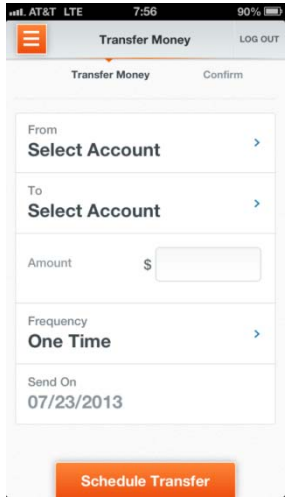
What Are Mobile Payments?

- Proposed definition:
  - A mobile payment is an exchange of monetary value which is effected between two parties where at least one of the parties is using a handheld mobile device.

Examples of “Mobile Payments” Today

- To the consumer, each of these are “payments”





Authentication for Payments

- What authentication occurs with a cash payment?

- Is the *customer* asking for stronger authentication?
- What specific problems are we looking to address?
- Who benefits?
- Why do we care?

How Do We Authenticate Today?

Payment Type	Authentication schemes
Cash	Physical possession
ACH	Bank's FFIEC authentication protocol
Wire	Up front vetting; multi-party approval; fax or call; UCC4 contract
Credit	Physical possession; signature; NAP; CVV
Debit	Physical possession; PIN
Check (EPO)	Bank's FFIEC authentication protocol; UCC4 contract

What of the above are truly authenticating the identity of the PERSON who is involved in the transaction?

Beneficial Characteristics of “Mobile”

- Processor
- Storage
- Connection
- Display
- Input
- Sensors

- User *wants* to carry the device
  - Users are quite adaptable

Mobile Payment Challenges

- Access at a distance
  - Unlike cash, once an payment mechanism gets "connected" it can be attacked from anywhere
- Velocity
  - Once an attack vector is identified, the speed with which nefarious actors can work their craft is greatly increased
- Little opportunity for "separation of duties"
  - Must protect items stored on the device

Two Sided Exchange

- Authentication considerations are as great for the payee as the payor

- Payee authentication may occur less frequently, but represents greater dollar volume

Scope

- Is all functionality available for all scenarios?
- What are constraints?
  - Timing? Value? Location? Connection?

- Who is responsible?
  - For what?

Contactless in a Mobile Context

- NFC has proven successful in card format
- NFC in mobile devices a young market
  - Global sales of handsets featuring NFC reached 140 million in 2012 (Berg Insight) of over 6 billion devices
    - And how many POS devices can read NFC?
- Existing wallet attempts clearly “R1.0”
  - Remember EMV

- Lots of opportunity!

Questions To Ask

- Who?
  - Who is allowed to pay? Who is responsible for doing the authentication of the payor?
- What?
  - What is being authenticated? A particular person? Control of device? Control of app? Availability of funds?
- When?
  - At what point does the authentication take place?
- Where?
  - Mobile app or web? At check-out, before or after?
- How?
  - What authentication mechanisms are being employed? Somethings you know/have/are?

What is the Attack Surface?

- What are the particular concerns for a given scheme?
- What is the fail over process?
- How much effort is involved to perpetrate the attack?
- When will the attack be discovered?

- Think like a bad guy

Solutions

What will likely work	What will likely not work
Schemes which give consumer control	Extend internet password
Layering (but not too inconvenient)	Social credentials
Passive authentication elements	Biometric as sole authenticator
Risk managed techniques	Multi-factor times multi-relationship
Privacy aware solutions	Heavy federation
Aggregated services	

It Is All About the User

- Remove the “groan factor”!

- Must balance security with east of use
- Users are adaptable – to a point
  - Proliferations of varying approaches frustrating
  - Give users a cohesive experience
- Authentication does not stand alone; still have to manage risk

- Users likely do not want to tie their payment capabilities to a 2 year phone contract

Industry Leadership

- What can regulators/lawmakers do?
  1. Measure performance
     - What is dollar value of risk?
  2. Consistent regulatory framework for payments
     - Baseline expectations across payment type
  3. Regulatory roadmap
     - Regulate for today, plan for tomorrow
  4. Coordinate with FCC
     - Rulemaking moving counter to securing platform

What do these have in common?

Small Decisions Can Have Big Impact

Questions?

- Otherwise, on with the day!

AUTHENTIFY®

www.authentify.com

Connect with us!

@Authentify Authentify, Inc. AuthentifyInc Authentify

For more information contact:

Peter Tapling
Authentify, Inc.
peter.tapling (at) authentify.com
+1-773-243-0322