

# Payment Fraud Trends & EMV Migration: What Small Businesses Need to Know

Katy Jacob

Payments Information Consultant  
Federal Reserve Bank of Minneapolis

Mary Hughes

Senior Payments Information Consultant  
Federal Reserve Bank of Minneapolis



U.S. Small Business Administration Webinar  
September 22, 2015

# Discussion Topics

- Payments Fraud Landscape
- Understanding Your Risk
- Fraud by Payment Type
- EMV Migration

## Disclaimer

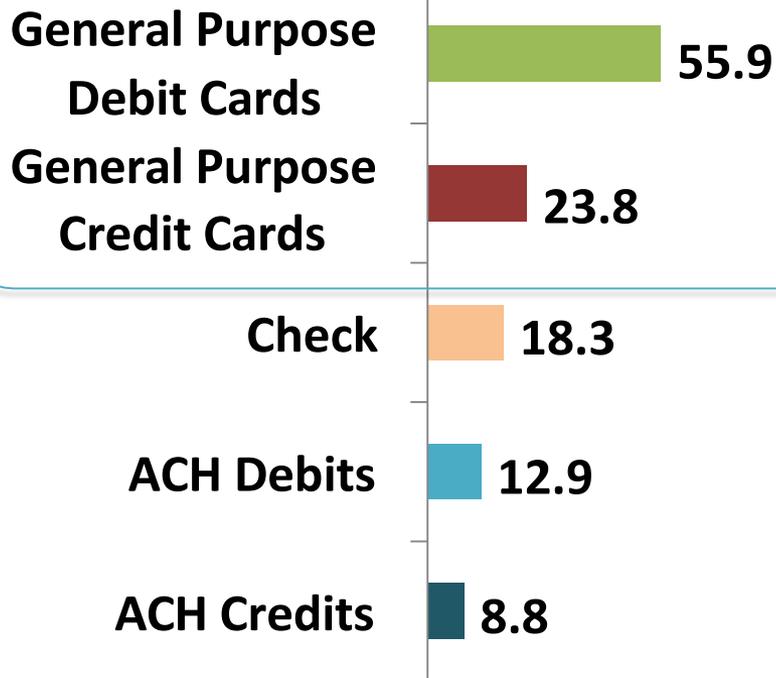
The opinions expressed are those of the individual presenters & not those of the Federal Reserve System, the Federal Reserve Bank of Minneapolis, or the U.S. Small Business Administration

# Payments Fraud Landscape

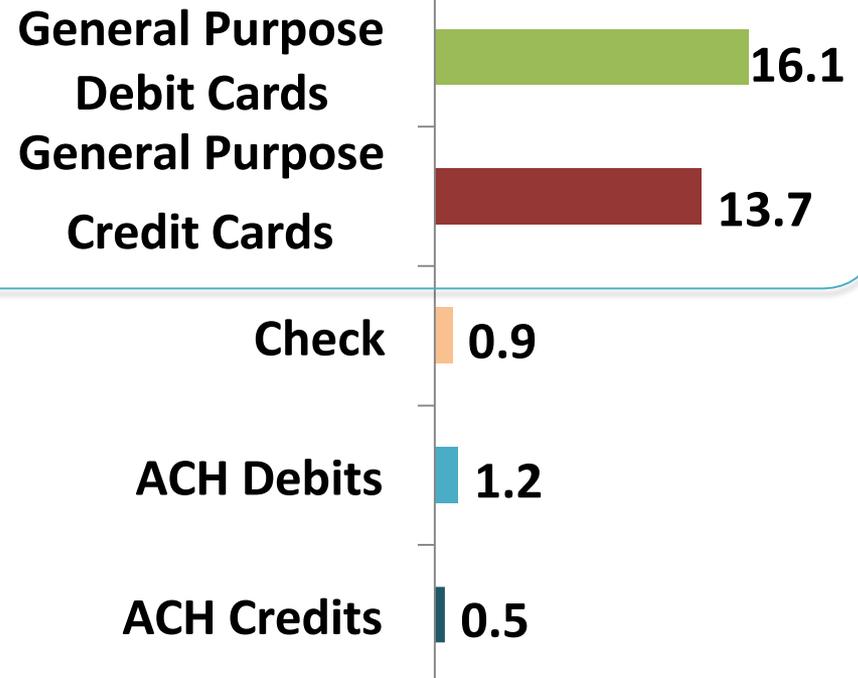


# U.S. Card Total Volume Is High & So Is Fraud Volume

## Transaction Volume 119.7 Billion



## Unauthorized\* Volume 32.3 Million



Source: 2013 Federal Reserve Payments Study

\*Data reflects unauthorized third-party fraud before chargebacks or recoveries

# Card Is Small in Total Value But Highest in Terms of Fraud Value

## Transaction Value \$174.7 Trillion

## Unauthorized Value \$6.4 Billion

General Purpose  
Credit Cards  
General Purpose  
Debit Cards

\$2.2

\$2.6

General Purpose  
Credit Cards  
General Purpose  
Debit Cards

\$2.3

\$1.8

Check

\$25.9

ACH Debits

\$66.7

ACH Credits

\$77.4

Check

\$1.1

ACH Debits

\$0.8

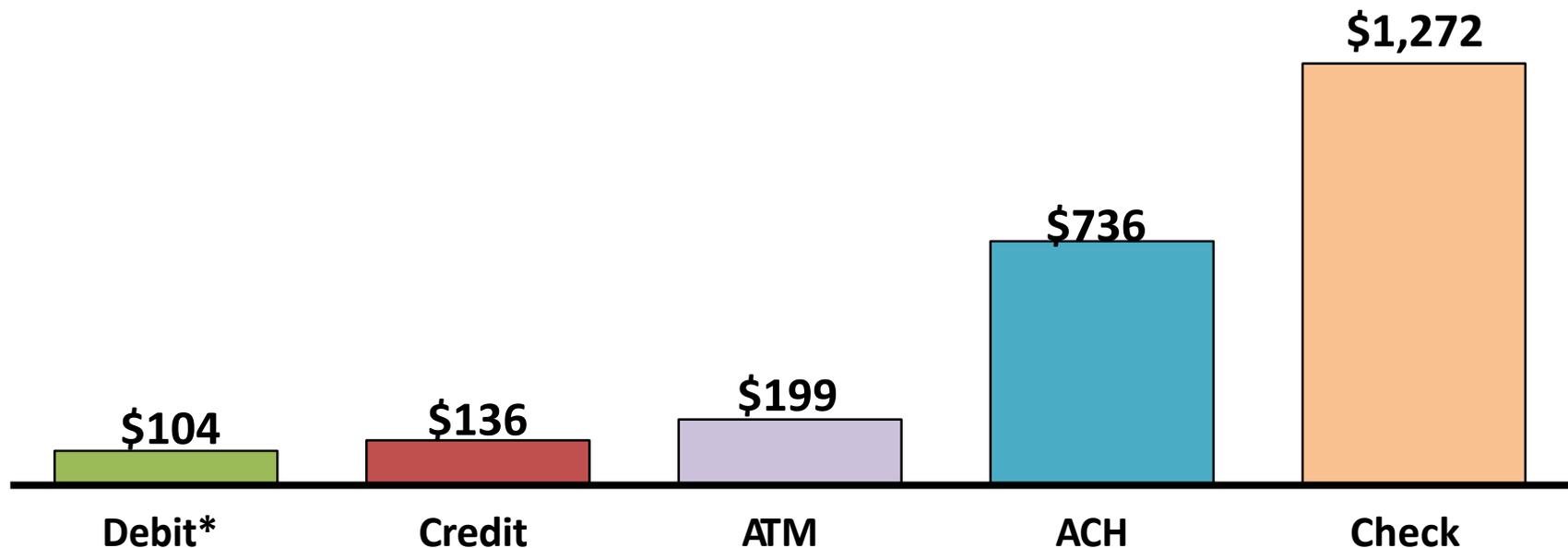
ACH Credits

\$0.4

Source: 2013 Federal Reserve Payments Study

# Checks Had Highest Average Value of Unauthorized Transactions

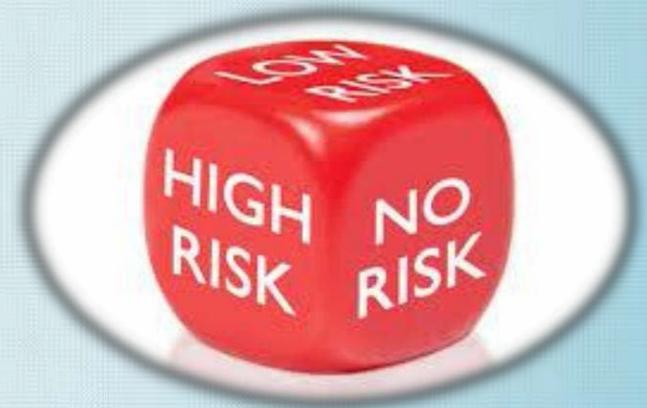
Average value of unauthorized transactions in 2012



\*Debit card includes prepaid cards

Source: 2013 Federal Reserve Payments Study

# Understanding Your Risk



# Completing a Risk Assessment

- Three basic components
  - Know your customers, vendors & suppliers
    - Who do you conduct payment transactions with?
  - Probability of fraud attempts by payment type
  - Dollar impact of successful fraud



# Who's on the Hook for Fraud Liability



## Understanding fraud liability

- Liability for payments fraud is governed by laws, regulations, & private contracts
  - Potential liability when a consumer is involved
- Liability varies by payment instrument, &
- It is complicated by market dynamics & innovation
  - Divergent case law makes it hard to know with certainty who is liable for payments fraud: check images, account takeover
  - “Remote” payments may change the nature of liability: card not present (CNP) fraud
- Practical matter of recovering lost funds & timing of recovery

# Main Barriers to Fraud Mitigation

Main Barriers	Non-FS* (N=154)
Lack of staff resources	55%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	53%
Consumer data privacy issues / concerns	25%
Corporate reluctance to share information due to competitive issues	36%
Cost of implementing commercially available fraud detection tool / service	8%

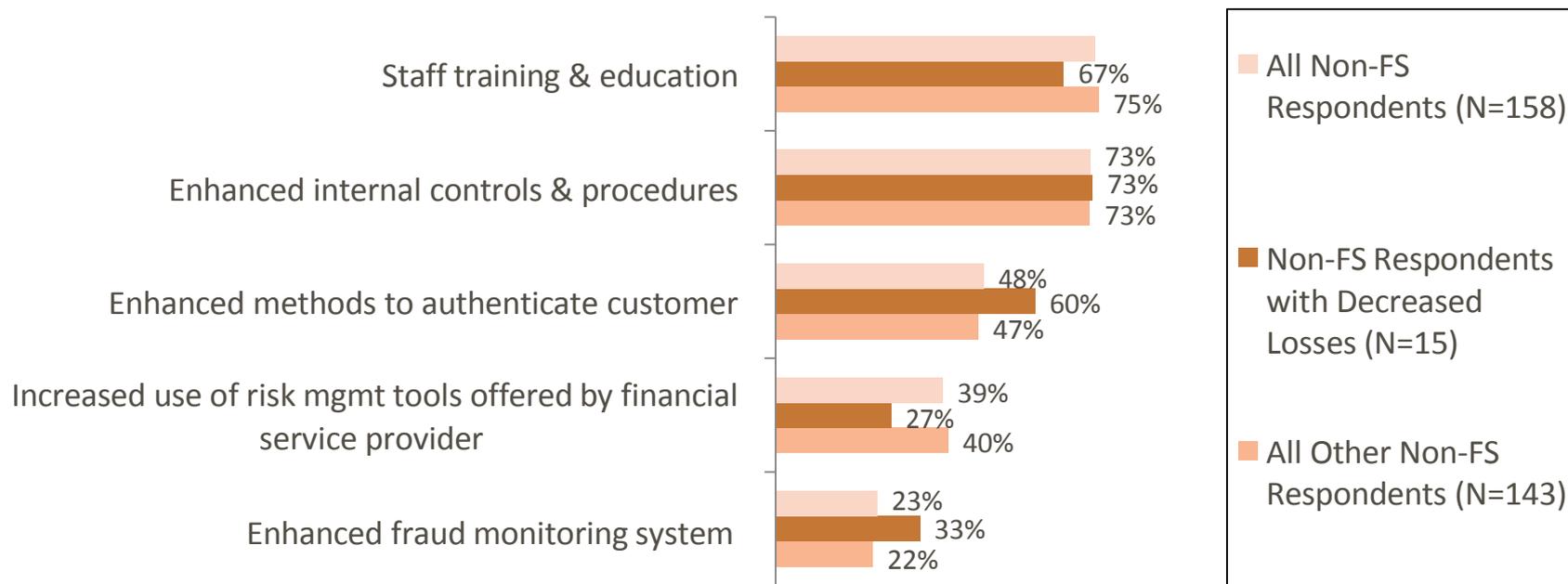
Source: Federal Reserve 2014 Payments Fraud Survey - Summary of Consolidated Results.

\* Non-FS= Non-Financial Services Companies

# Controlling Fraud Losses: Non-FS Respondents

- Nearly 3 out of 4 Non-FS respondents report changes made to staff training & education & internal controls & procedures

**Key Changes Made to Payments Risk Management Practices  
by % of FS Respondents that Made Changes**



Source: Federal Reserve 2014 Payments Fraud Survey - Summary of Consolidated Results

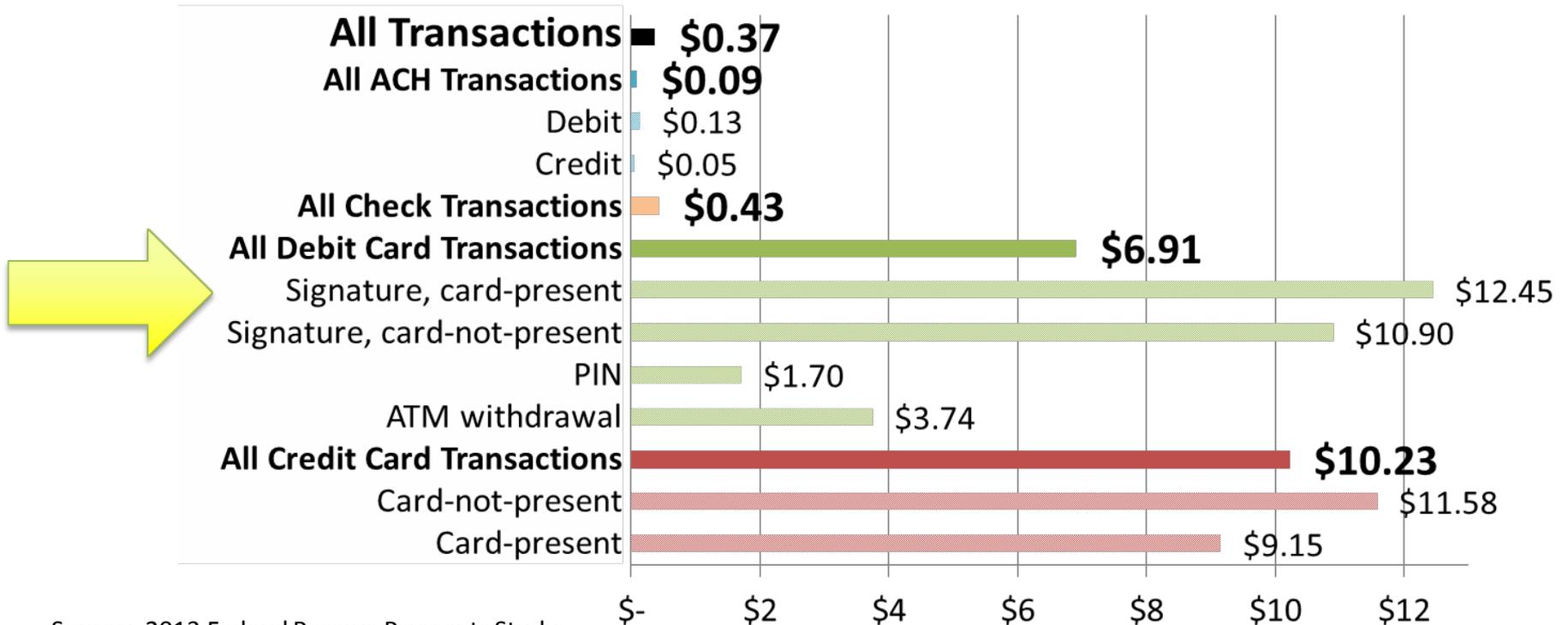
# Fraud by Payment Type



# Unauthorized Transactions by Payment Method

- What payment type has the highest loss rate due to unauthorized transactions?

Loss per \$10,000 Spent



Source: 2013 Federal Reserve Payments Study

# Check Fraud



- Low barriers & costs to entry
- Account & other information needed is accessible
- Attributes of paper facilitate fraud
- Common types of fraud: Counterfeits, Alterations, Forgeries
- Remote deposit capture may create new fraud risks
  - Check frauds may be harder to detect—e.g., physical alterations such as check “washing” may be obscured by imaging process
  - Certain check security features may be lost through imaging process
  - Insider fraud potential may increase—e.g., presenting checks more than once, stealing personal information on checks

# Card Fraud



## Common Types of Card Fraud

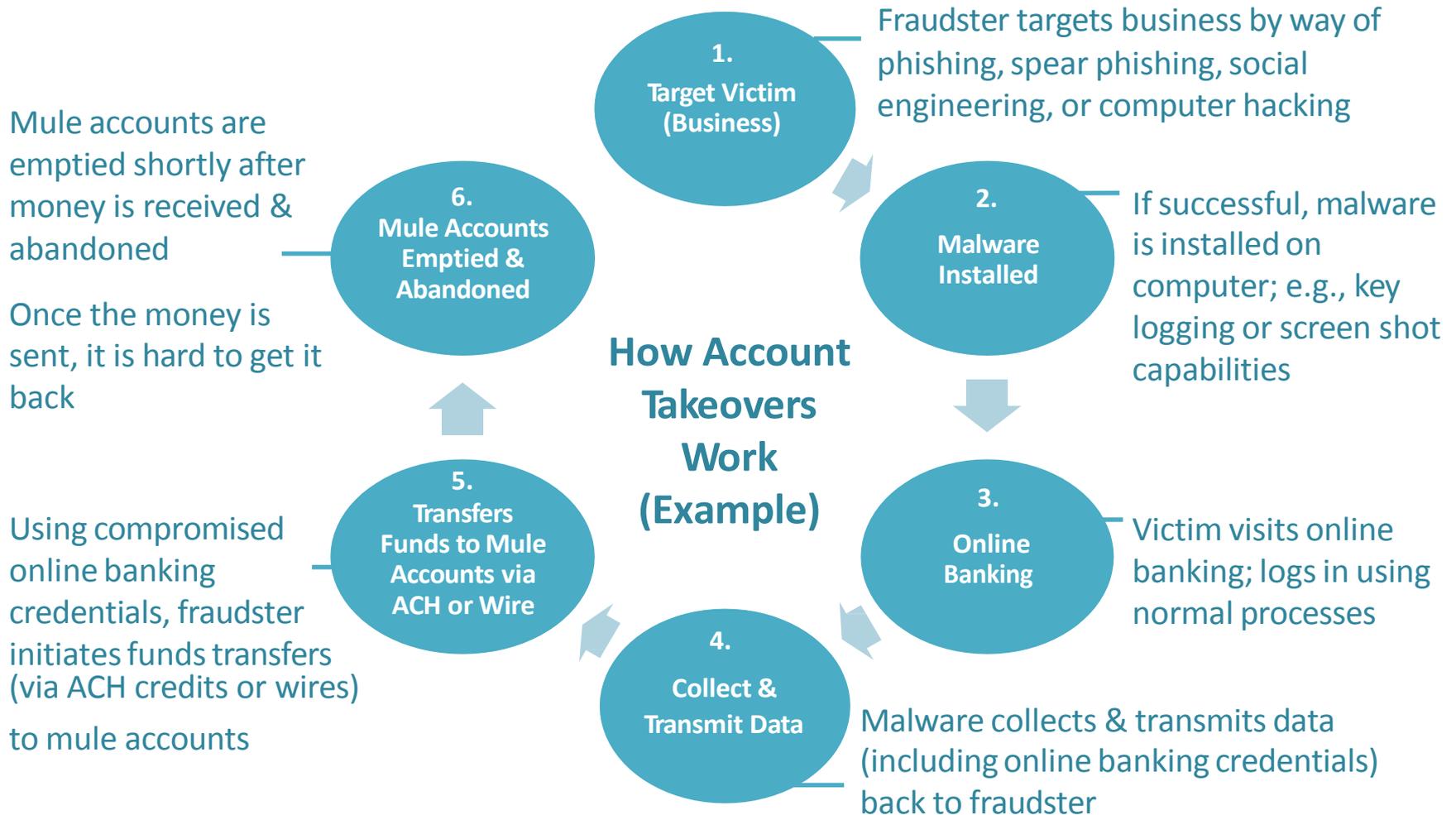
- On purchasing cards (p-cards) or commercial cards
  - Employee misuse
  - Use of lost or stolen cards
    - Fraudsters may “ping” an account with a small purchase to see if the transaction goes through before escalating the attack
  - Counterfeit cards used online or at point of sale
- When accepting card payments
  - Counterfeit, lost, or stolen cards
    - Used at point of sale (card present)
    - Used online (card-not-present)

# Fraud Involving ACH that Affects Businesses



- Unauthorized debits to accounts
  - Your business's account information is obtained & used to create unauthorized ACH debits against your business bank account
- Check positive pay rejects represented as ACH debits
- Email scams, e.g., reverse phishing
  - A fraudster impersonates one of your vendors
  - Business receives email instructing a change to the payment account information for your outgoing payments to that vendor
  - Your accounts payable sends ACH credits to updated account without realizing it is a fraud scheme
- Fraudulent claims of unauthorized debits
  - Your customer claims they did not authorize payment via an ACH debit
- Origination of fraudulent ACH items by an insider
- Account takeovers that issue fraudulent ACH payments

# Fraud Involving ACH that Affects Businesses – Account Takeovers



# Points of Interaction Are Potential Points of Compromise



## Online

Phishing  
Spear Phishing  
Spoofing  
Hacking  
Social Engineering

## Telephone

Smishing  
Vishing  
Impersonator Fraud  
Social Engineering  
Eavesdropping

## Physical Hardware, Documents, & Mail

Device Tampering  
Dumpster Diving  
Theft  
Employee Misuse

# What Should Small Businesses & Others Be Doing?

- Ensure fraud prevention & detection is an organizational objective
  - Complete a risk assessment, set policies, establish procedures, monitor compliance, & take action on exceptions
- Leverage cost-effective tools & processes to address vulnerabilities
  - Talk to your banker about using their free or low cost fraud monitoring tools
- Educate & train employees on fraud prevention



# What Should Small Businesses & Others Be Doing?

- Check accounts daily
- Secure your bank account information, lock up paper documents, limit access to sensitive online data
- Use strong passwords & change them often
- Monitor & measure fraud attempts & losses
- Update defenses; best practices today may not be best practices tomorrow



# EMV Migration



# What Is EMV?

- EMV (Europay, MasterCard & Visa) is a set of global proprietary specifications for credit & debit payment cards, point-of-sale terminals & card transaction processing networks based on “smart chip” card technology



EMV chip cards use an embedded microprocessor for payment transactions

# Main Benefits of Chip Cards

- Improved usability of U.S. cards in worldwide EMV markets
- Reduced POS counterfeit fraud
- Harder to skim data from EMV transactions
  - Chips authenticate card readers & EMV cards to one another at POS, & can detect tampering
- Reduced fraud from foreign EMV cards used as mag stripe cards in U.S.

# How EMV Works

- Integrated Circuit Card (ICC)
- Designed to be used as contact or contactless
- Not just a card but a system
  - Terminals
  - New messaging data
  - New application logic
  - New configuration settings
- All stakeholders affected
  - Issuers
  - Merchants
  - Processors
  - Networks
  - Cardholders



# U.S. EMV Migration Roadmaps

## Key Dates

	October 2012	April 2013	October 2013	April 2015	October 1, 2015	October 2016	October 2017
Visa	PCI audit relief	Acquirers & processors required to support merchant acceptance of EMV transactions		3 <sup>rd</sup> party ATM acquirer processors & sub-processors required to support EMV data	Card-present counterfeit liability takes effect excluding automated fuel dispensers (AFD)		ATM liability shift Card-present counterfeit liability takes effect for automated fuel dispensers
MasterCard			Account Data Compromise (ADC) relief (50%)		ADC relief (95% - 100%) Lost or stolen liability shift	ATM liability shift	Lost or stolen liability shift for AFD
Discover			PCI audit relief				
American Express			PCI reporting relief				

# EMV Liability Shifts

- **October 2015**
  - Card-present liability shift for most merchants not including automated fuel dispensers (AFD)
  - Lost or stolen liability shift (MasterCard, Discover & American Express)
- **October 2016**
  - Liability shift for ATM owners (MasterCard)
- **October 2017**
  - Liability shift for ATM owners (Visa)
  - Liability shift for AFDs (Visa, MasterCard, Discover & American Express)
  - Lost or stolen liability shift for AFD (MasterCard, Discover & American Express)



# Status of EMV Adoption - Issuance Is at a Tipping Point

- At end of 2014, about 120 million of the 1.2 billion credit & debit cards in circulation in the U.S. were EVM-compliant
- EMV Migration Forum estimates the U.S. will have 600 million chip cards in circulation by end of 2015
  - Ontrack Advisory predicts between 40 to 50% of U.S. cards will be EMV-ready by October



# Status of EMV Adoption – Merchant Acceptance



- Figures vary...
  - Merchant Advisory Group estimates that about 20% of merchants POS terminals will be EMV-capable by end of 2015; Ontrack Advisory pegs this at 25 to 30%
  - Visa estimates 47% of POS terminals are activated to accept EMV cards
- Larger retailers are installing EMV POS terminals



Visa presentation at June 2015 EMV Migration Forum meeting

# Small Merchants Lag in EMV Readiness

- Only half of smaller businesses are aware of October liability shift
  - Only 31% say their existing credit card processing system accepts chip-enabled cards
  - 29% plan to equip yet this year
  - 40% have no plans

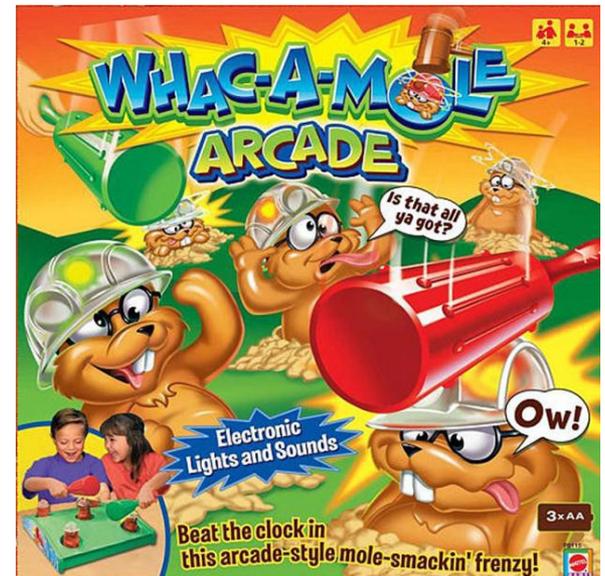
Source: Wells Fargo/Gallup Small Business Index July 2015

# EMV is an Opportunity for SBs

- Helps SB owners benefit from the latest enhancements in payment technology while also meeting the needs of their customers who want to best protect themselves from fraud
- Reduces counterfeit fraud in card-present transactions
- Avoids assuming liability shift
- Reduces PCI reporting cost
- May help protect against fraud loss shifts to U.S. from countries adopting EMV
- Supports standard card payment methods across countries
- Ability to accept EMV cards from international travelers

# How Does EMV Impact Card-Not-Present Transactions?

- Once EMV takes hold, other countries have seen fraudsters target on-line transactions, perpetrate elaborate ATM fraud schemes, & attack markets without chip-&-PIN
- Chip cards don't protect **card-not-present transactions** in the e-commerce space; other solutions must be applied
  - Fraud attacks shift to most vulnerable channels
  - Merchants bear losses due to CNP fraud



# Fighting CNP Fraud

- **Authentication Methods & Tools**
  - **Endpoint Security** (device level authentication)
  - **One-Time Password** (valid for only one transaction or online session)
  - **Randomized Pin Pad** (scrambles the key pad & captures XY coordinates)
  - **Biometrics** (iris, retina, hand, voice, fingerprint, etc.)
  - **3D Secure** (enables real-time cardholder authentication during an online transaction)
  - **Tokenization** (replaces personal account number with surrogate values)
  - **Proprietary Approaches** (e.g., membership, registration in customer loyalty programs)

# Next Steps for Small Biz

- Talk to your card provider and/or payment processor
- Research low-cost options - costs will vary depending on the type of business & your system needs, but there are many affordable hardware solutions
- Explore new payment technologies on the horizon such as contactless payments that allow consumers to pay with a smartphone linked to a credit card
- Learn more by checking out [sba.gov/EMV](https://www.sba.gov/EMV) and <https://www.minneapolisfed.org/about/what-we-do/payments-information>

# Resources



- Talk to your banker
  - Visit your bank’s website for tips on preventing payments fraud
- The Remittance Coalition <https://fedpaymentsimprovement.org/get-involved/remittance-coalition/>
  - Small Business Payments Toolkit <https://fedpaymentsimprovement.org/wp-content/uploads/small-business-toolkit.pdf>
  - Payment Types Explained [https://www.minneapolisfed.org/~media/files/about/what-we-do/remittance%20coalition/asbdcd\\_july\\_2013\\_payment\\_types\\_explained.pdf?la=en](https://www.minneapolisfed.org/~media/files/about/what-we-do/remittance%20coalition/asbdcd_july_2013_payment_types_explained.pdf?la=en)
- Federal Reserve Bank of Minneapolis [www.minneapolisfed.org](http://www.minneapolisfed.org) & our Payments Information Resources <https://www.minneapolisfed.org/about/what-we-do/payments-information:>
  - 2014 Federal Reserve Payments Fraud Survey – Regional & Consolidated Results
  - Industry & Government Information-Sharing Resources Related to Payments Fraud
  - Payments Fraud Liability Matrix
- America’s SBDC [www.americassbdc.org](http://www.americassbdc.org)
- Federal Reserve System 2013 Federal Reserve Payments Study [http://www.frbservices.org/communications/payment\\_system\\_research.html](http://www.frbservices.org/communications/payment_system_research.html)
- Improving the U.S. Payment System <https://fedpaymentsimprovement.org/>
- Learn about EMV cards at the card brands websites (Visa, MasterCard, Discover & American Express)
- Public resources available from EMV Migration Forum at:
  - <http://www.emv-connection.com/emv-resources/>
  - [www.gochipcard.com](http://www.gochipcard.com)

# Resources, continued



- National Association of Credit Management [www.nacm.org](http://www.nacm.org)
- Association for Certified Fraud Examiners [www.acfe.com](http://www.acfe.com)
- Association for Financial Professionals [www.afponline.org](http://www.afponline.org)
- Board of Governors of the Federal Reserve System [www.federalreserve.gov](http://www.federalreserve.gov)
- Federal Financial Institutions Examination Council [www.ffiec.gov](http://www.ffiec.gov)
- Multi-State Information Sharing & Analysis Center [www.msisac.org](http://www.msisac.org)
- Financial Services Information Sharing and Analysis Center (FS ISAC)  
<http://www.fsisac.com/>
  - Alert: Securing Merchant Card Payment Systems from the Risks of Remote Access 7/7/2015 <https://www.fsisac.com/sites/default/files/news/Alert%20--%20Securing%20Merchant%20Terminals%20Remote%20Access%20FINAL%207%20July%202015.pdf>
  - Fraud Alert: Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses 6/19/2015  
[http://www.fsisac.com/sites/default/files/news/BEC\\_Joint\\_Product\\_Final.pdf](http://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf)
- International Association of Financial Crimes Investigators [www.iafci.org](http://www.iafci.org)
- National Automated Clearing House Association [www.nacha.org](http://www.nacha.org)
- U.S. Small Business Administration landing page on EMV: [www.sba.gov/emv](http://www.sba.gov/emv)

# Questions

