# Fight or Flight

## Fraud in Payments 2017

**Lee Wetherington**

Director of Strategic Insight

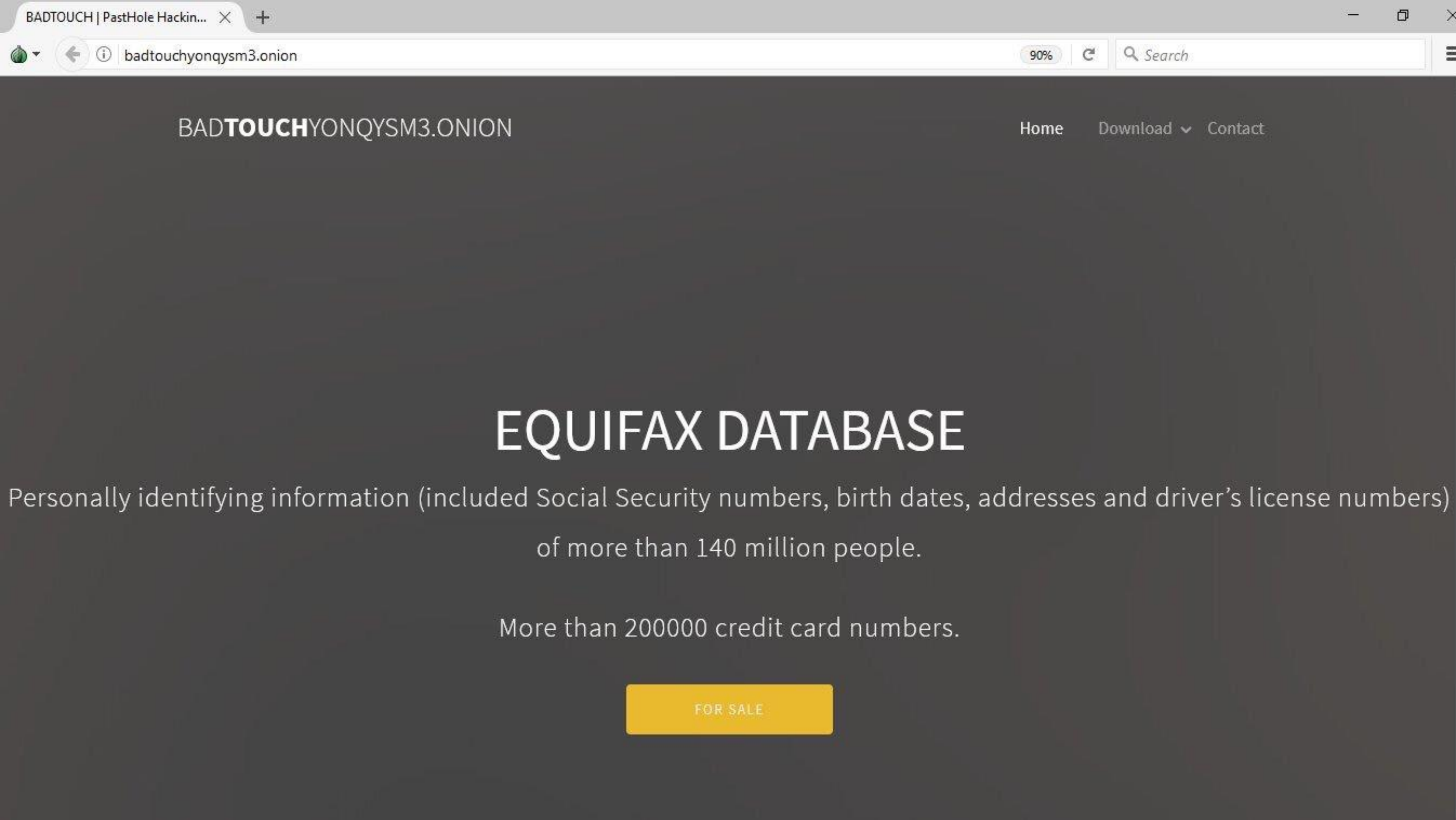
Jack Henry & Associates, Inc.®

@leewetherington

Wisconsin Bankers ASSOCIATION

**Secur-I.T. Conference 2017**

# Who was part of the Equifax breach?



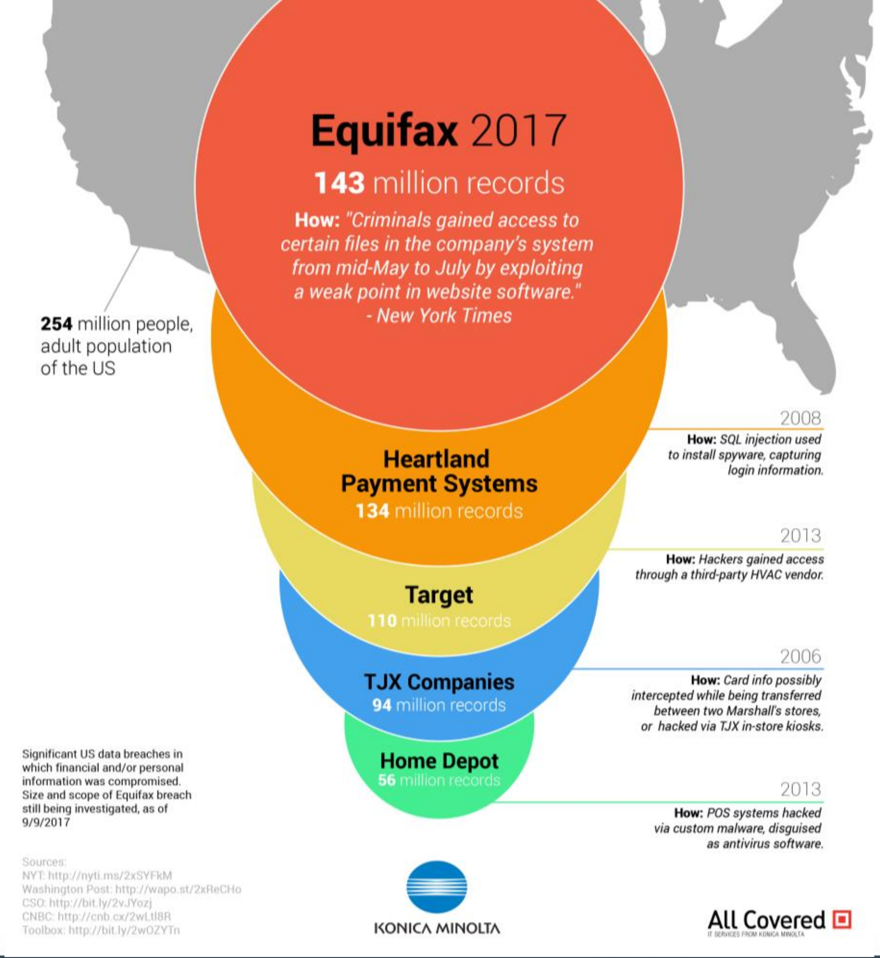
# EQUIFAX DATABASE

Personally identifying information (included Social Security numbers, birth dates, addresses and driver's license numbers) of more than 140 million people.

More than 200000 credit card numbers.

# How big was Equifax hack?

- Over half of U.S. adults affected.



**Equifax** 2017

**143** million records

**How:** *"Criminals gained access to certain files in the company's system from mid-May to July by exploiting a weak point in website software." - New York Times*

**254** million people,
adult population
of the US

**Heartland Payment Systems**
**134** million records

2008
**How:** *SQL injection used to install spyware, capturing login information.*

**Target**
**110** million records

2013
**How:** *Hackers gained access through a third-party HVAC vendor.*

**TJX Companies**
**94** million records

2006
**How:** *Card info possibly intercepted while being transferred between two Marshall's stores, or hacked via TJX in-store kiosks.*

**Home Depot**
**56** million records

2013
**How:** *POS systems hacked via custom malware, disguised as antivirus software.*

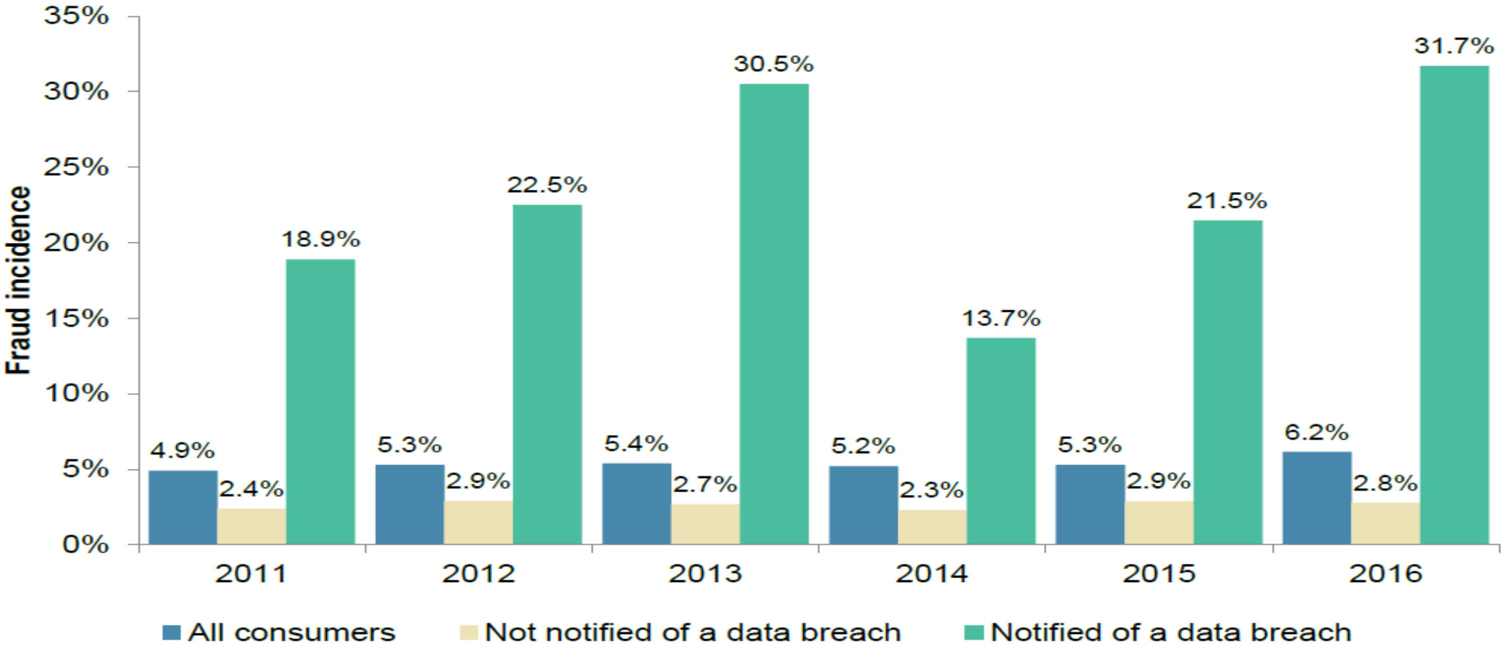
Significant US data breaches in which financial and/or personal information was compromised. Size and scope of Equifax breach still being investigated, as of 9/9/2017

Sources:
NYT: http://nyti.ms/2xSYFkM
Washington Post: http://wapo.st/2xReCHo
CSO: http://bit.ly/2vJYozj
CNBC: http://cnb.cx/2wLtl8R
Toolbox: http://bit.ly/2wOZYTn

SOURCE:https://www.allcovered.com/learning/wp-content/uploads/equifax3_whiteBG.png

# Fraud incidence for breach victims reaches all-time high

Figure 21: Fraud Incidence by Breach Notification Status, 2011–2016



Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

# Who thinks privacy is still a thing?

Who has Bluetooth enabled on your phone right now?

Mobile bankers that download apps from unofficial app sources:

**7.7 Million**

Assets at risk from mobile banking Trojan infections:

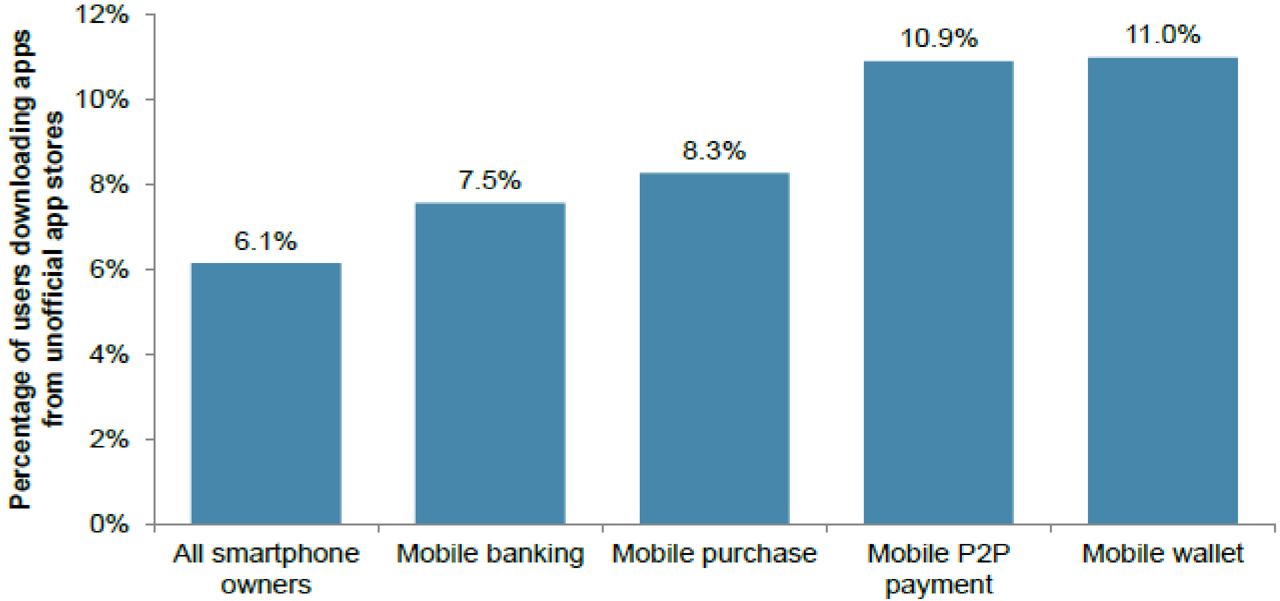
**$221.5 Billion**

SOURCE: Javelin's "2017 Mobile Banking Malware Report"

# Mobile Banking Users at Risk for Malware Infection

**Mobile Wallet, P2P Users at Risk for Malware Infection From Third-Party Apps**

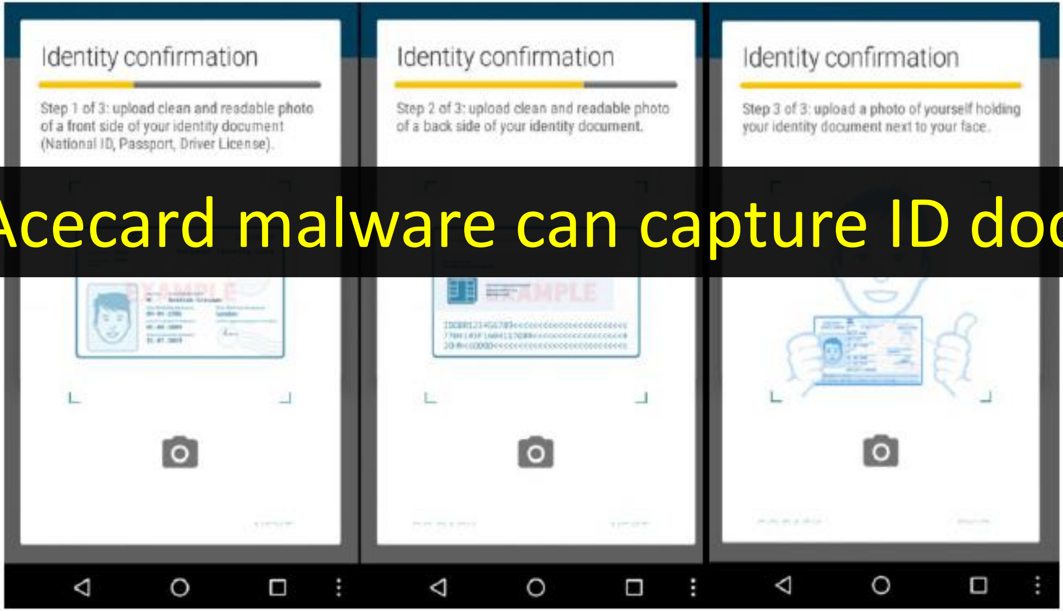
Figure 1. Use of Unofficial App Stores by Users of Mobile Financial Services



SOURCE: Javelin's “2017 Mobile Banking Malware Report”

# Overlay Attacks Mimic Legitimate App Interfaces

Acecard Document Capture Overlay Screens



Identity confirmation

Step 1 of 3: upload clean and readable photo of a front side of your identity document (National ID, Passport, Driver License).

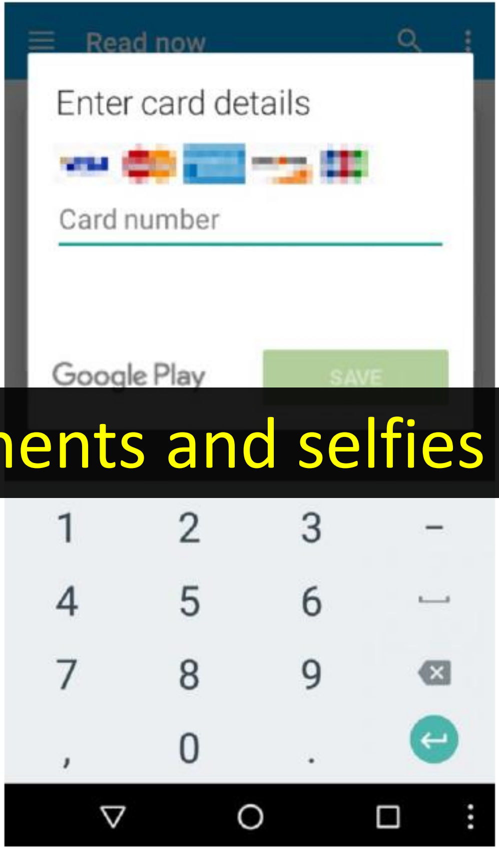
Identity confirmation

Step 2 of 3: upload clean and readable photo of a back side of your identity document.

Identity confirmation

Step 3 of 3: upload a photo of yourself holding your identity document next to your face.

Image courtesy of McAfee



Enter card details

Card number

Image courtesy of McAfee

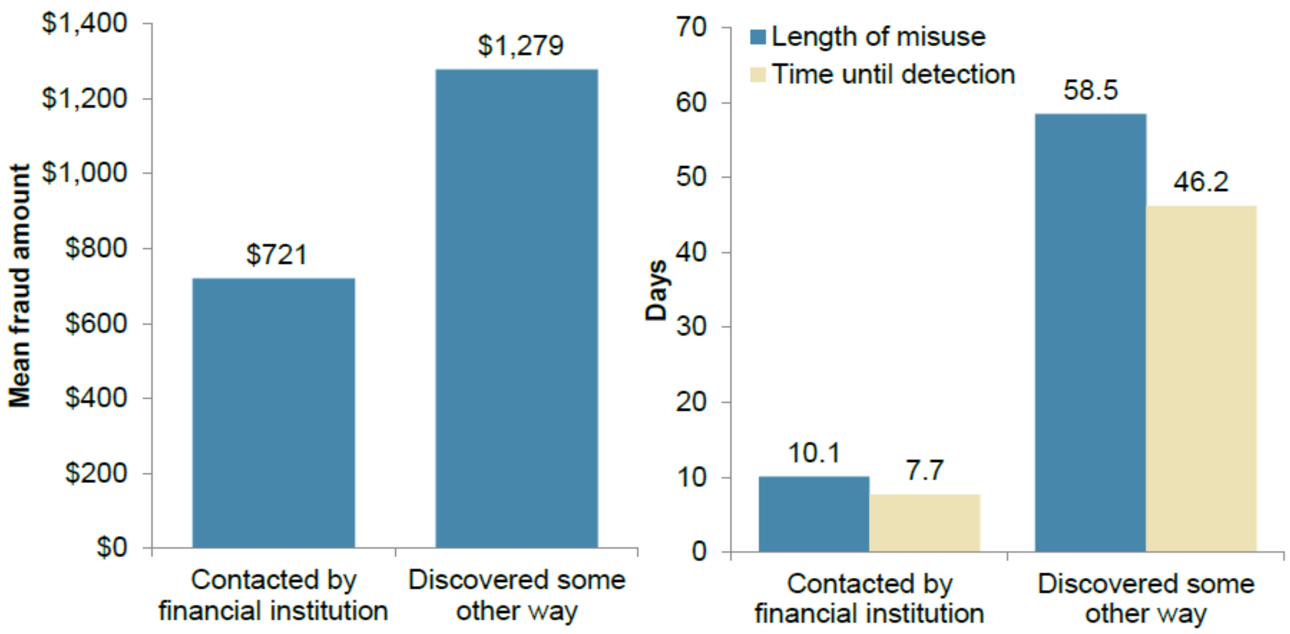
Acecard malware can capture ID documents and selfies

SOURCE: Javelin's "2017 Mobile Banking Malware Report"

# Without bank detection, fraud lingers & losses go up

**Without FI Detection, Fraud Lingers and Grows More Expensive**

Figure 4. Mean Fraud Amount, Length of Misuse, Time to Detection, by Means of Discovery



SOURCE: Javelin's "2017 Mobile Banking Malware Report"

# Mobile Malware: What You Should Know

- Sideloading is primary infection pathway
- Mobile wallet and mobile P2P users are 75% more likely to expose themselves by way of sideloading
- Overlay attacks are the newest, most sophisticated threat
- Existing malware can subvert most prevalent authentication methods in U.S., SMS messages/OTPs
- Some malware encourages victims to log into mobile banking to expedite theft of credentials (e.g. Marcher)

SOURCE: Javelin's "2017 Mobile Banking Malware Report"

# Solutions: Practical and Aspirational

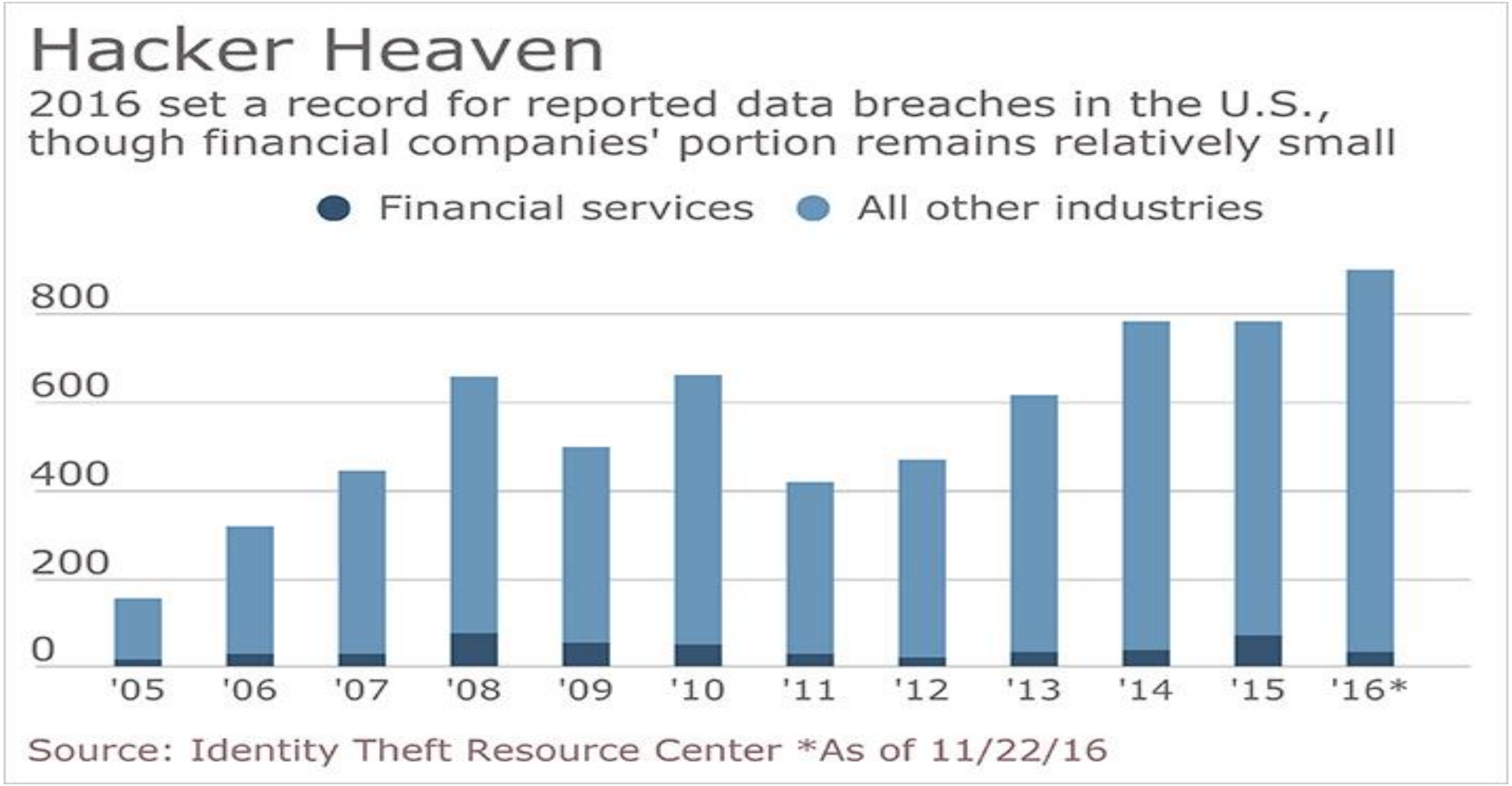
- Make mobile banking apps detect mobile malware
  - e.g., Google Safety Net API detects whether device has been rooted, infected or has dangerous apps.
  - Overlay detection in mobile banking app?
- Integrate device-integrity info into risk-based authentication
- Educate customers on mobile security best practices
  - Risks of sideloading; identifying risky apps; anti-malware

SOURCE: Javelin's "2017 Mobile Banking Malware Report"

# Solutions: Practical and Aspirational, cont'd

- Use personalization of login pages to thwart overlays
- Move away from passwords and text-based authentication
  - Toward biometrics (TouchID) and behaviometrics
- Migrate away from SMS one-time passwords (OTPs)
  - The more prevalent malware becomes, the more vulnerable use of OTPs becomes

SOURCE: Javelin's "2017 Mobile Banking Malware Report"



Hacker Heaven

2016 set a record for reported data breaches in the U.S., though financial companies' portion remains relatively small

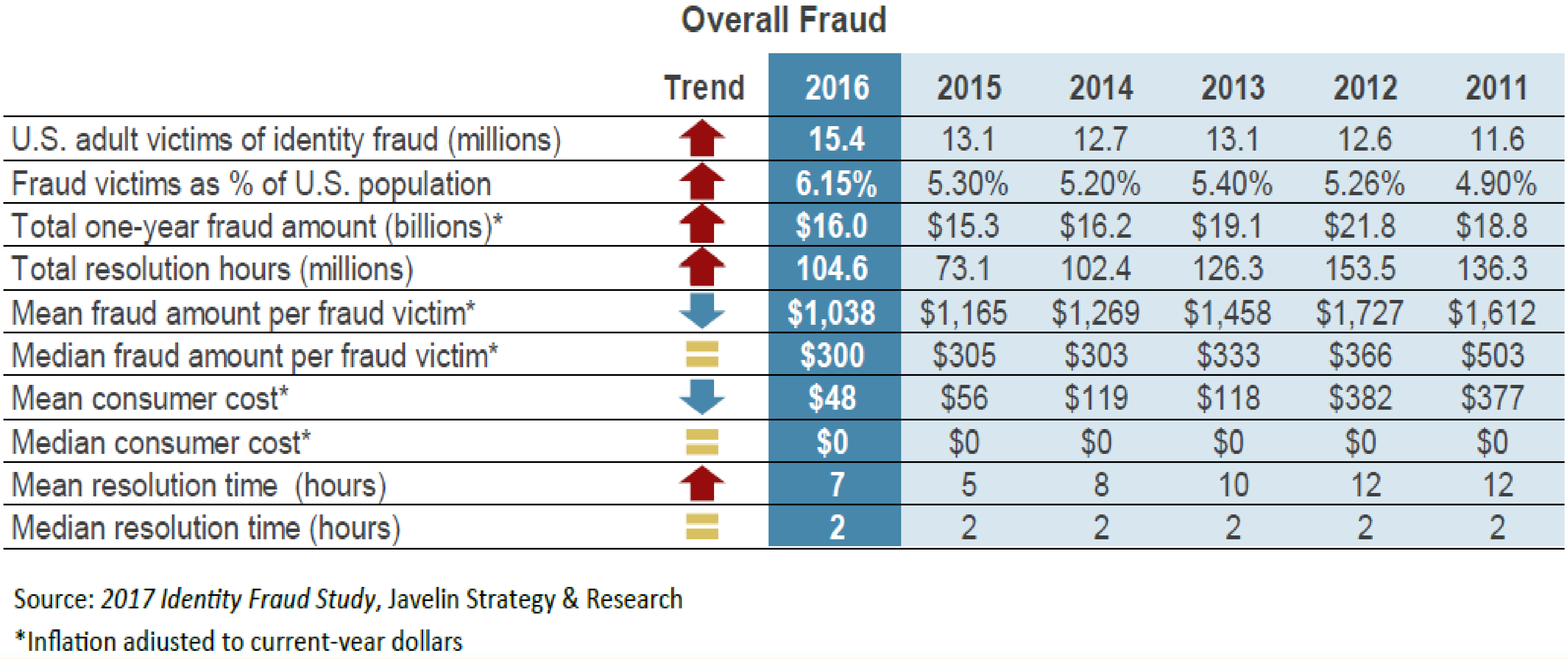
Source: Identity Theft Resource Center *As of 11/22/16

SOURCE: “BIG IDEAS FOR 2017: Customer Data Is a Liability
By Marc Hochstein; American Banker; January 5, 2017

Privacy is not a thing.

PII is dead…as a stand-alone authenticator.

# Identity Fraud Trends in the U.S. (Javelin)



## Overall Fraud

| | Trend | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 |
|---|---|---|---|---|---|---|---|
| U.S. adult victims of identity fraud (millions) | ↑ | 15.4 | 13.1 | 12.7 | 13.1 | 12.6 | 11.6 |
| Fraud victims as % of U.S. population | ↑ | 6.15% | 5.30% | 5.20% | 5.40% | 5.26% | 4.90% |
| Total one-year fraud amount (billions)* | ↑ | $16.0 | $15.3 | $16.2 | $19.1 | $21.8 | $18.8 |
| Total resolution hours (millions) | ↑ | 104.6 | 73.1 | 102.4 | 126.3 | 153.5 | 136.3 |
| Mean fraud amount per fraud victim* | ↓ | $1,038 | $1,165 | $1,269 | $1,458 | $1,727 | $1,612 |
| Median fraud amount per fraud victim* | = | $300 | $305 | $303 | $333 | $366 | $503 |
| Mean consumer cost* | ↓ | $48 | $56 | $119 | $118 | $382 | $377 |
| Median consumer cost* | = | $0 | $0 | $0 | $0 | $0 | $0 |
| Mean resolution time (hours) | ↑ | 7 | 5 | 8 | 10 | 12 | 12 |
| Median resolution time (hours) | = | 2 | 2 | 2 | 2 | 2 | 2 |

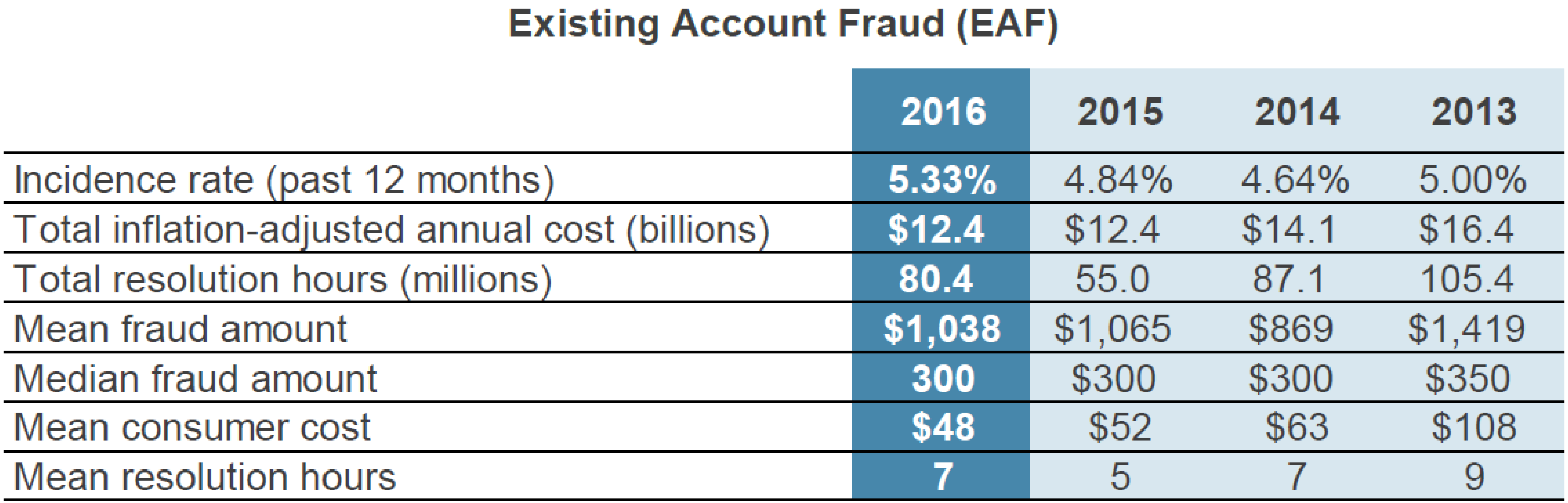
Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

*Inflation adiusted to current-vear dollars

# Fraud: What You Should Know

- Number of U.S. fraud victims at all-time high
- Last year was first time incidence of all fraud types increased (NAF, ECF, ENCF)
- Account Takeover (ATO) fraud jumped 36% last year, and ATO fraud losses increased 60%
  - Mobile phone account takeovers doubled last year
- Post-breach fraud incidences is at all-time high
  - 1 in 3 notified breach victims experience fraud within a year
- CNP fraud increases; does more damage than POS fraud

# Existing Account Fraud (EAF) ticks up, takes longer



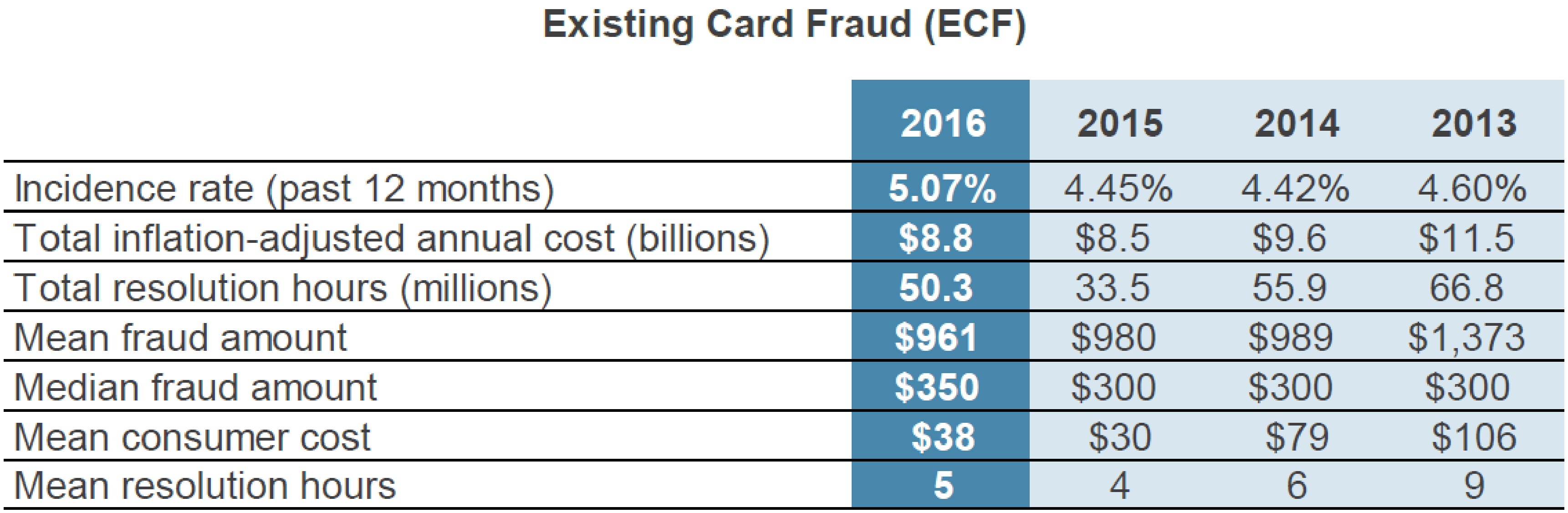
## Existing Account Fraud (EAF)

| | 2016 | 2015 | 2014 | 2013 |
|---|---|---|---|---|
| Incidence rate (past 12 months) | **5.33%** | 4.84% | 4.64% | 5.00% |
| Total inflation-adjusted annual cost (billions) | **$12.4** | $12.4 | $14.1 | $16.4 |
| Total resolution hours (millions) | **80.4** | 55.0 | 87.1 | 105.4 |
| Mean fraud amount | **$1,038** | $1,065 | $869 | $1,419 |
| Median fraud amount | **300** | $300 | $300 | $350 |
| Mean consumer cost | **$48** | $52 | $63 | $108 |
| Mean resolution hours | **7** | 5 | 7 | 9 |

Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

# What is the most prevalent type of payment fraud?

# Exiting Card Fraud (ECF) affects more than ever



### Existing Card Fraud (ECF)

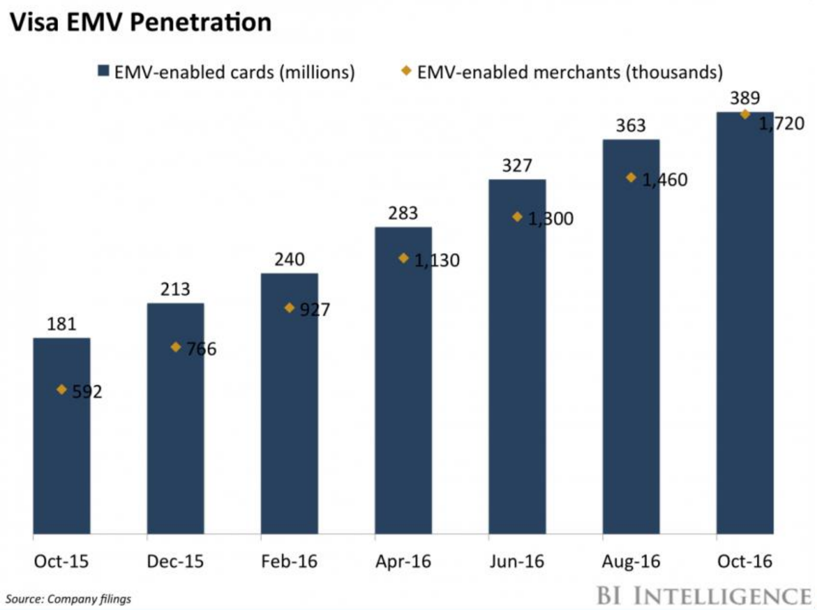
| | 2016 | 2015 | 2014 | 2013 |
|---|---|---|---|---|
| Incidence rate (past 12 months) | **5.07%** | 4.45% | 4.42% | 4.60% |
| Total inflation-adjusted annual cost (billions) | **$8.8** | $8.5 | $9.6 | $11.5 |
| Total resolution hours (millions) | **50.3** | 33.5 | 55.9 | 66.8 |
| Mean fraud amount | **$961** | $980 | $989 | $1,373 |
| Median fraud amount | **$350** | $300 | $300 | $300 |
| Mean consumer cost | **$38** | $30 | $79 | $106 |
| Mean resolution hours | **5** | 4 | 6 | 9 |

Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

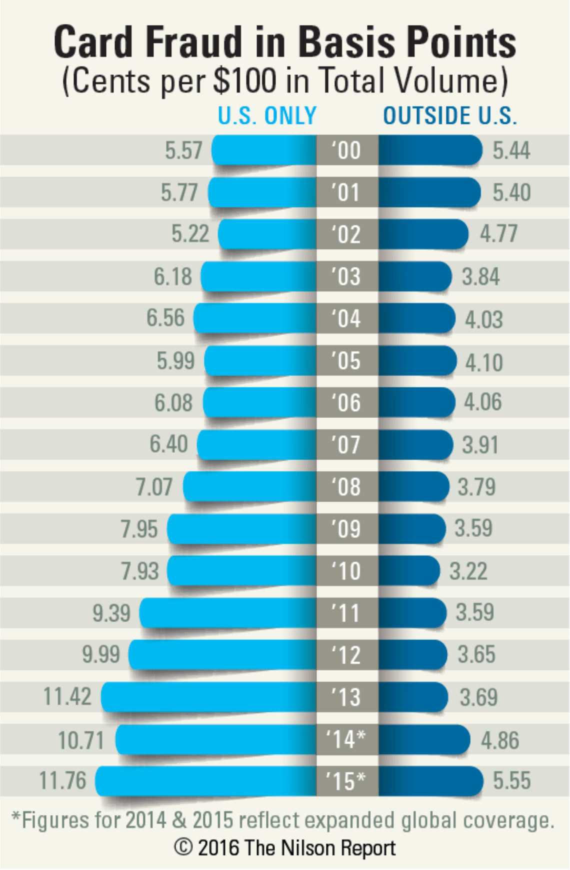
# Card Fraud

**Trends:**

- EMV card issuance and merchant acceptance is on the rise
- Increase in online fraud has become more prevalent


Visa EMV Penetration

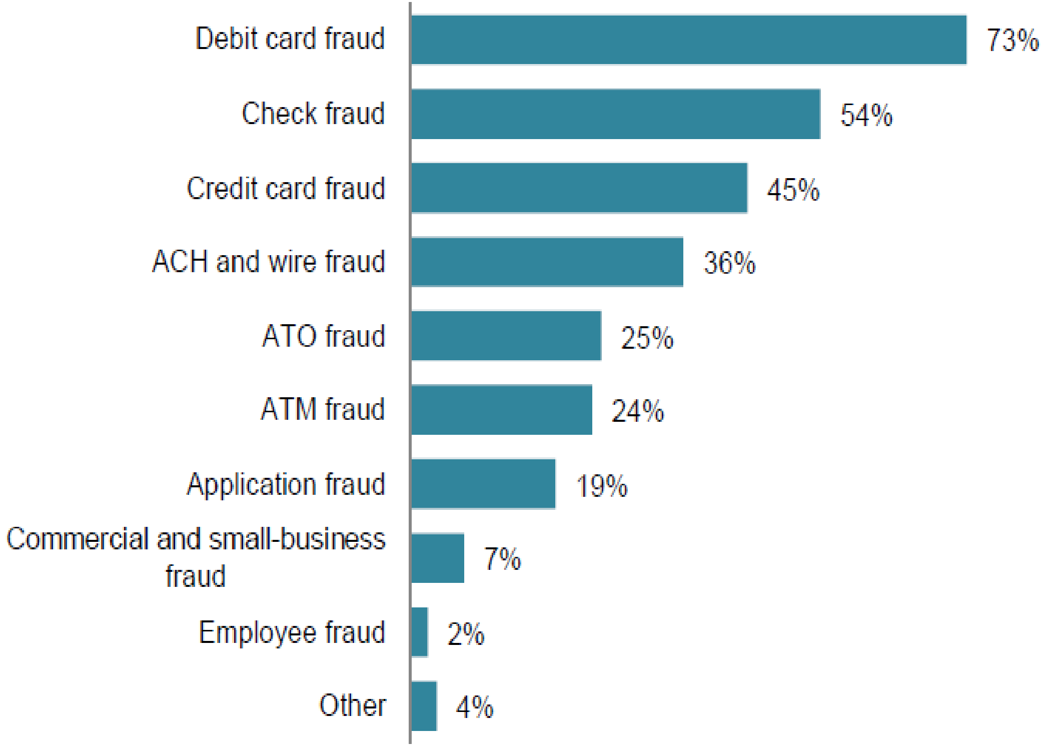
*Source: Company filings*


Card Fraud in Basis Points
(Cents per $100 in Total Volume)

*Figures for 2014 & 2015 reflect expanded global coverage.
© 2016 The Nilson Report

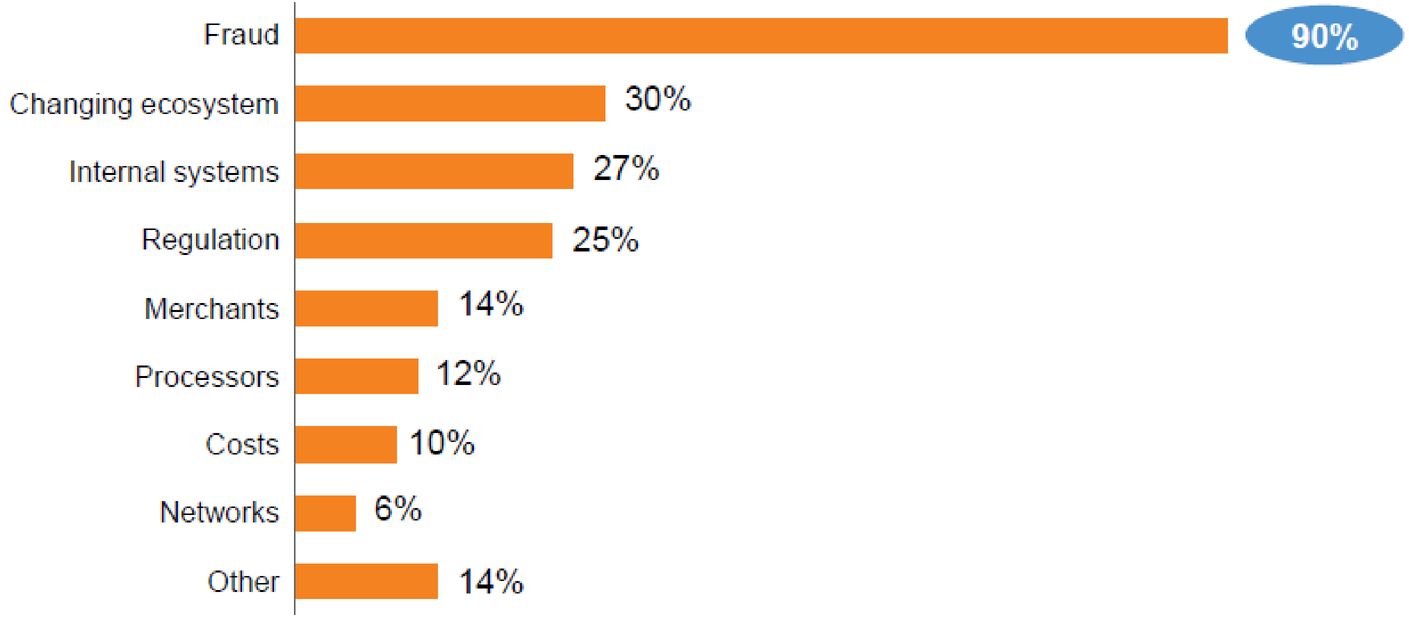
# Debit Cards Still Biggest Fraud Challenge

- What are the top 3 challenges you bank faces with regard to fraud threats?



SOURCE: Aite Group’s survey of 83 U.S. FI executives, March & April 2017

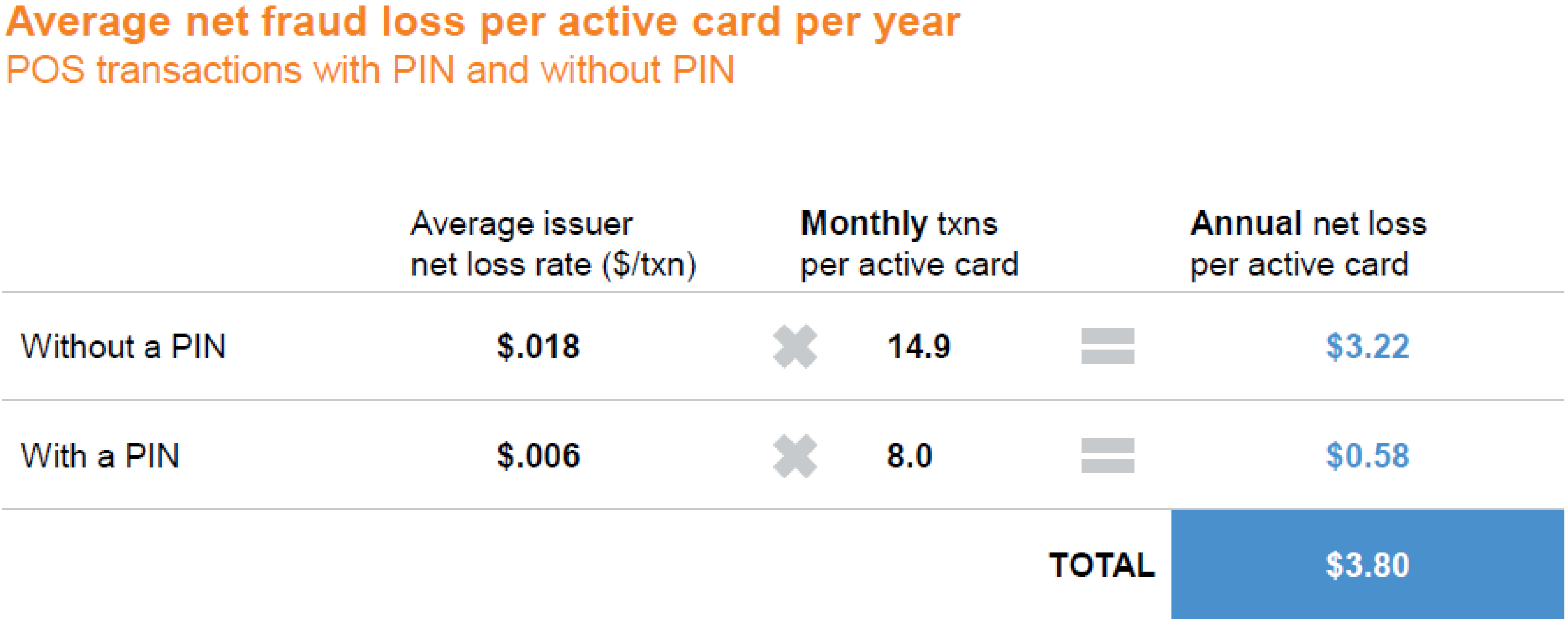
# Fraud is debit issuers biggest pain point



Note: “Other” includes time to implement plans, reporting, optimizing loyalty programs, and EMV reissue-driven volume loss

SOURCE: PULSE 2017 Debit Issuer Study

# Average debit card fraud losses per card per year



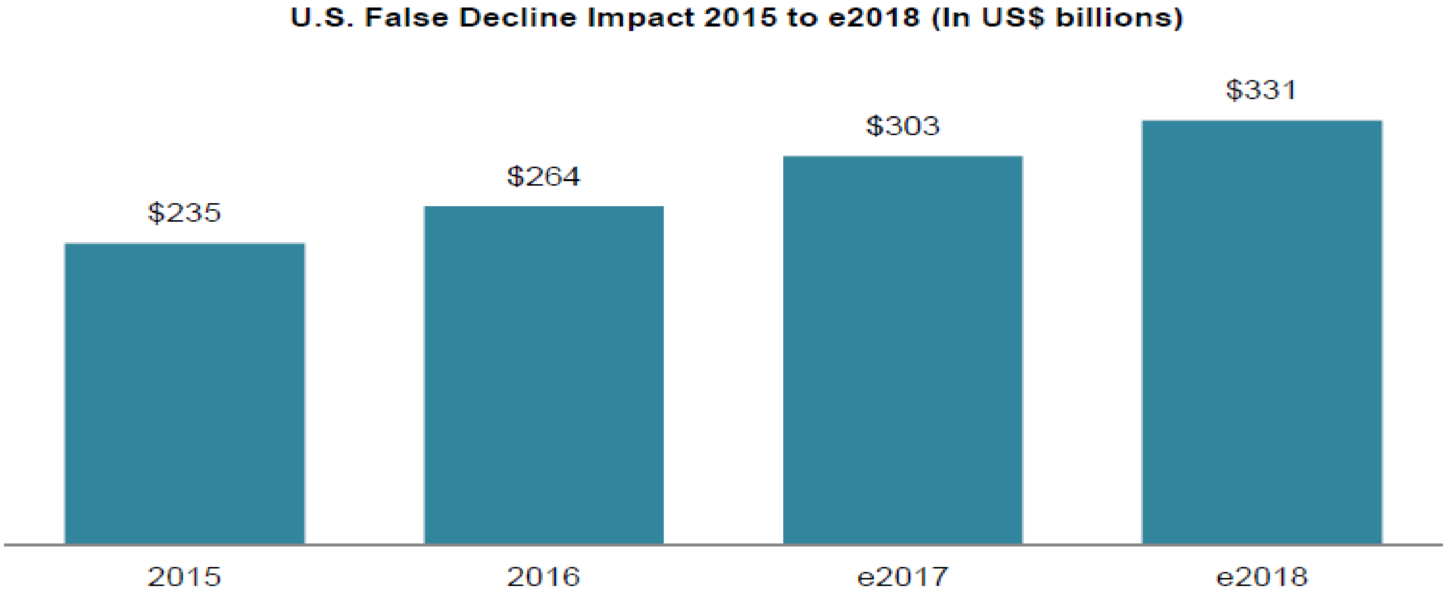
**Average net fraud loss per active card per year**

POS transactions with PIN and without PIN

| | Average issuer net loss rate ($/txn) | | Monthly txns per active card | | Annual net loss per active card |
|---|---|---|---|---|---|
| Without a PIN | $.018 | × | 14.9 | = | $3.22 |
| With a PIN | $.006 | × | 8.0 | = | $0.58 |
| | | | | TOTAL | $3.80 |

SOURCE: PULSE 2017 Debit Issuer Study

# False Decline Impact in the U.S.

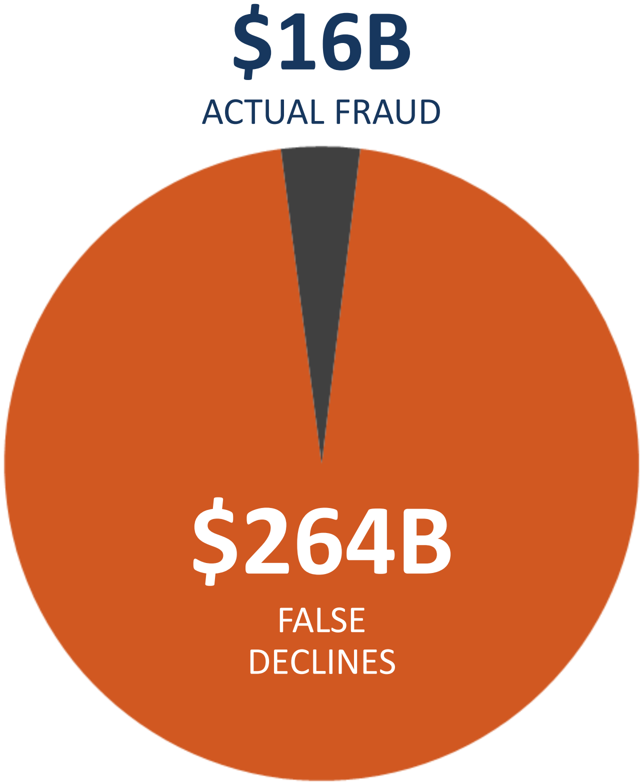


*Source: Aite Group*

# False Declines > Actual Fraud

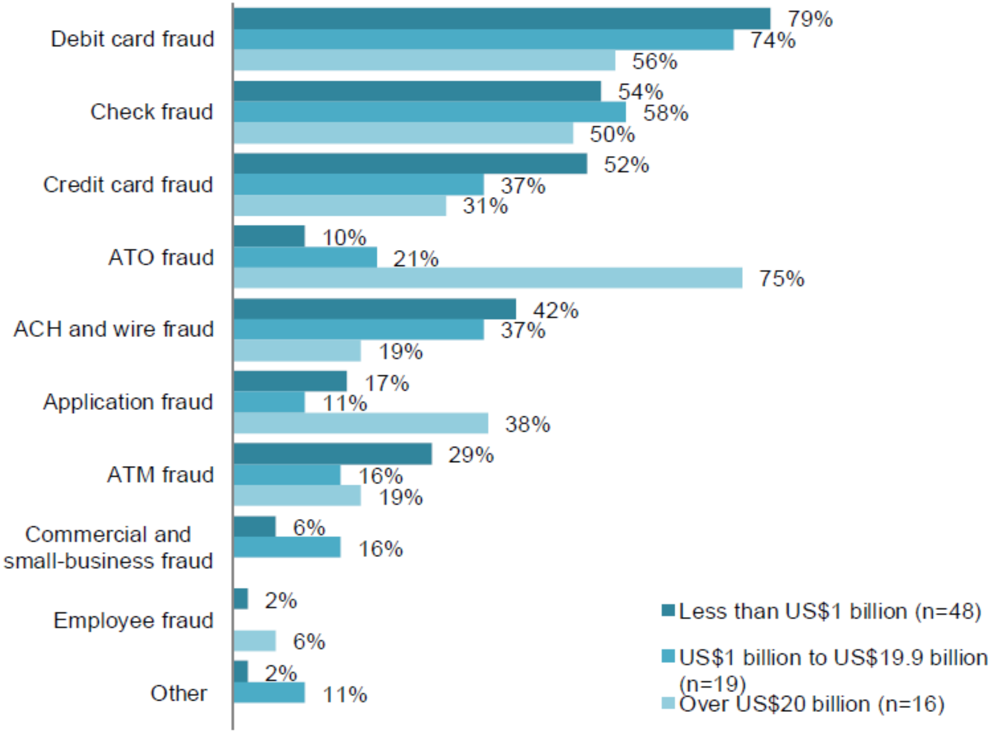
**U.S. issuers falsely declined $264B in card transactions in 2016:**
**16X actual fraud of $16B**

Javelin Strategy & Research & Aite Group



# Fraud Challenges by Asset Size

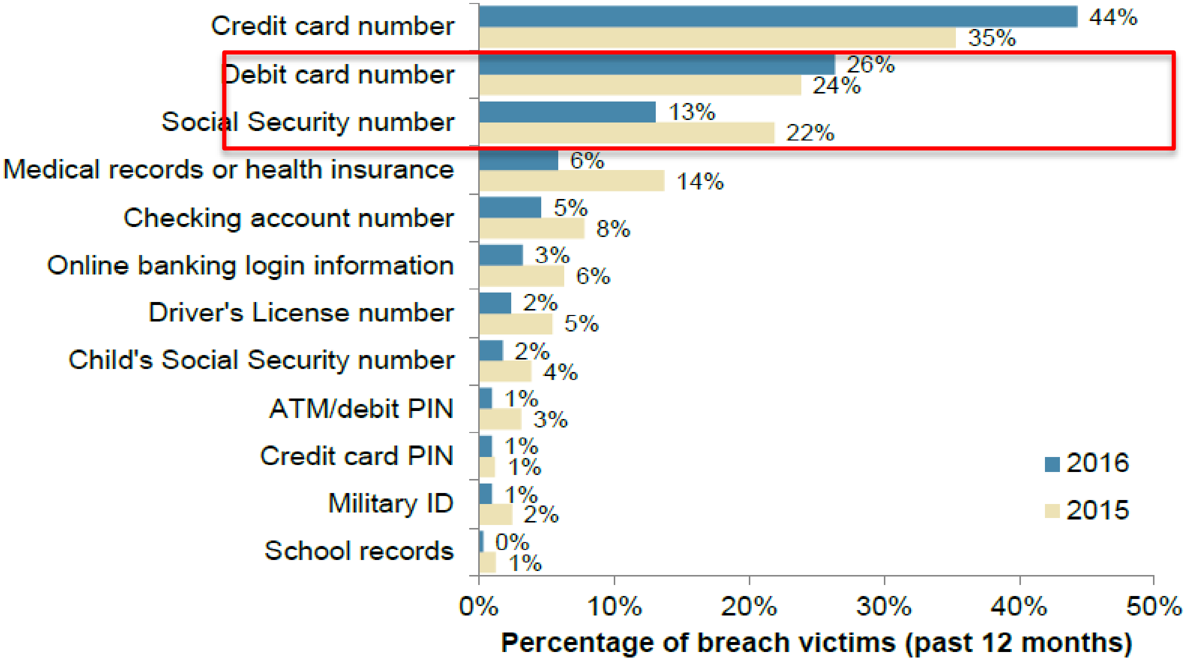
- ATO fraud and application fraud are disproportionately bigger challenges for the largest banks above $20B in assets.



SOURCE: Aite Group's survey of 83 U.S. FI executives, March & April 2017

# Credit Cards Still Most Compromised

Type of Data Breached Among Notified Fraud Victims, 2015-2016

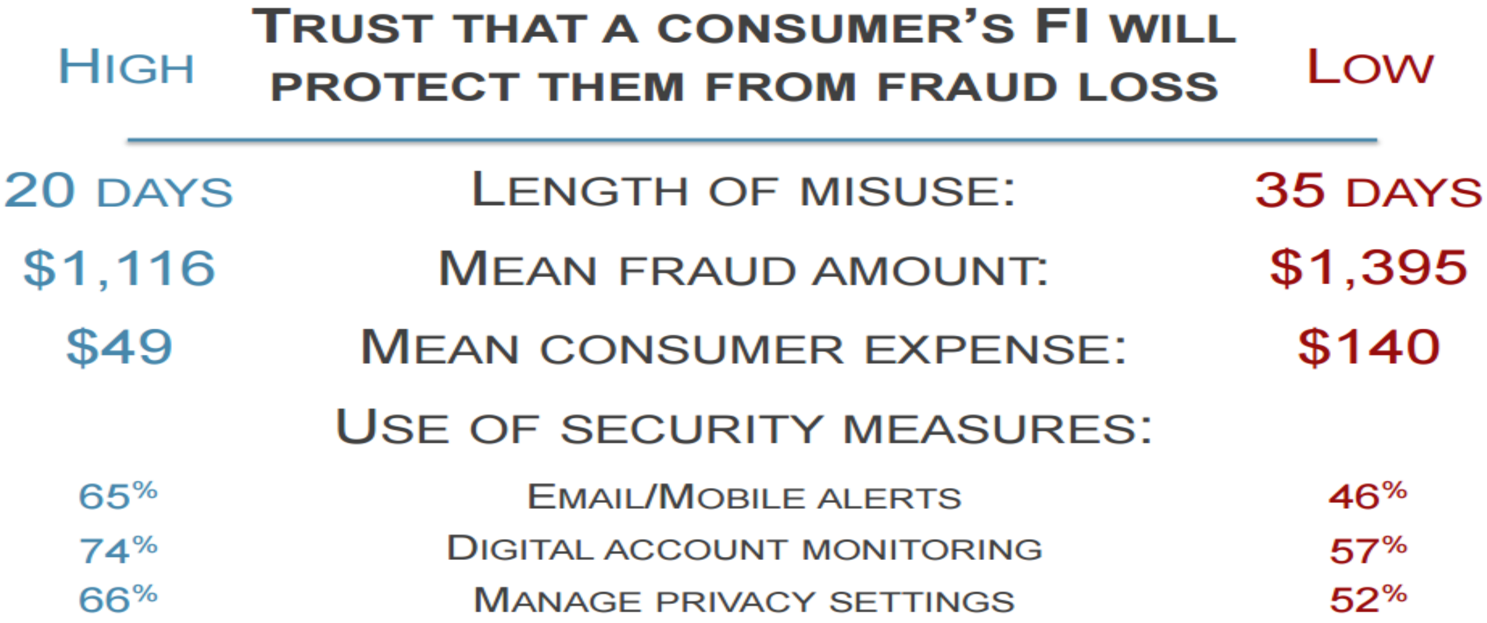


Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

©2017 Jack Henry & Associates, Inc.

# Poor Fraud Resolution = Big Problems

**Impact of Fraud Resolution Experience on Trust in FI, Willingness to Use Security Measures**



| High | Trust that a consumer's FI will protect them from fraud loss | Low |
|---|---|---|
| 20 days | Length of misuse: | 35 days |
| $1,116 | Mean fraud amount: | $1,395 |
| $49 | Mean consumer expense: | $140 |
| | Use of security measures: | |
| 65% | Email/Mobile alerts | 46% |
| 74% | Digital account monitoring | 57% |
| 66% | Manage privacy settings | 52% |

SOURCE: Javelin Strategy & Research; 2016 Identity Fraud: Fraud Hits An Inflection Point; February 2016

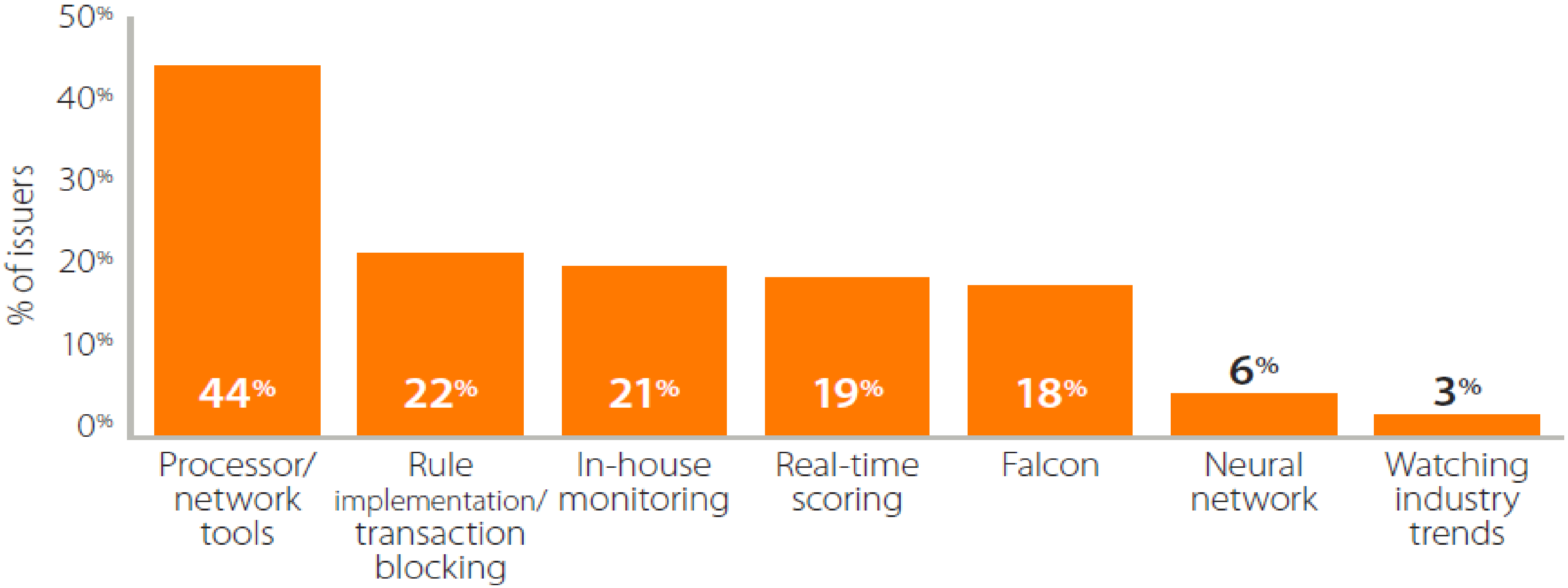
# What’s happening?

- **CNP fraud grows**
  - Driven by e-commerce growth and EMV shifting fraud from counterfeit fraud at POS to online card payments
- **Issuers tighten authorizations** in response
- Tighter authorizations **generate more false declines**
- **Issuer losses from improperly declined transactions** (plus reduced future spend from dissatisfied cardholders) **outpaces fraud losses 4-to-1**
  - 40% of declined cardholders abandon cards
  - Additional 25% reduce card usage
    - 11% drop in cardholder spending 3 months after decline
    - Spending remains 8% lower 6 months later

SOURCE: MasterCard Advisors, Security Matters, “How Much Does a Declined Transaction Intended to Prevent Fraud Really Cost?”

© 2017 Jack Henry & Associates, Inc.

# Debit Fraud Tools Used Now



*Note: Values do not add to 100 as each issuer could provide multiple answers*

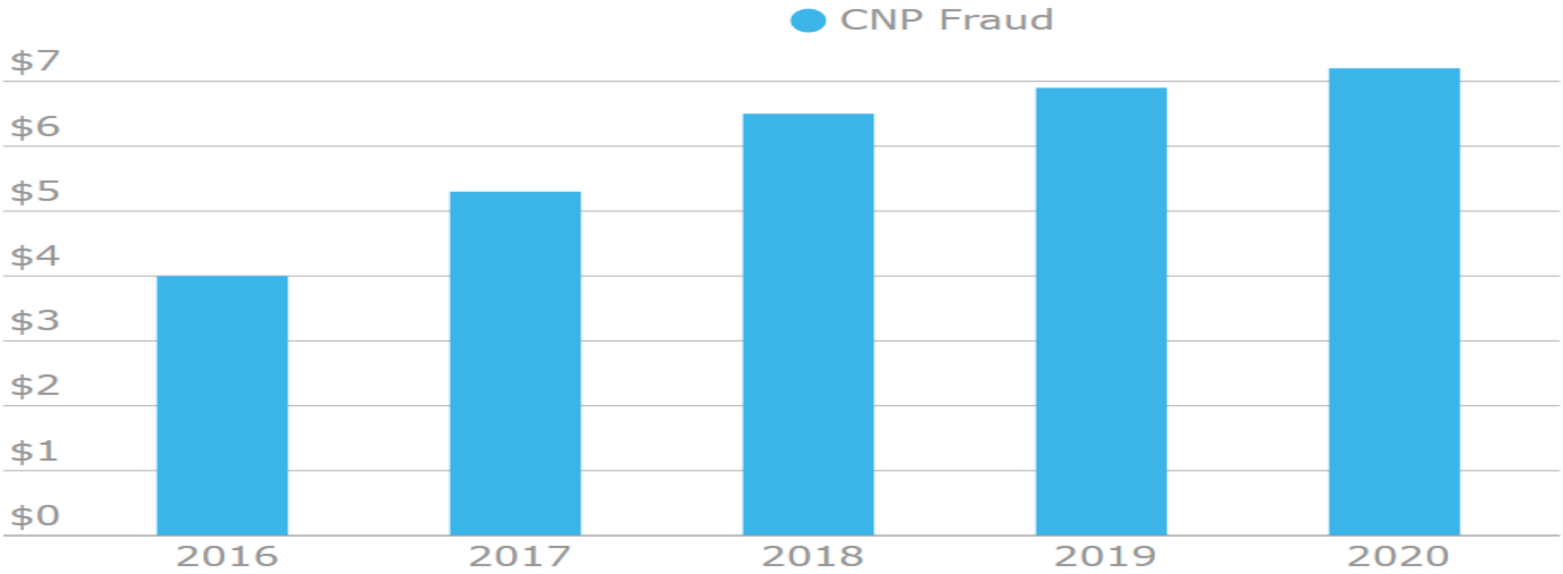
SOURCE: PULSE 2016 Debit Issuer Study Executive Summary

© 2017 Jack Henry & Associates, Inc

# CNP Fraud Will Continue to Grow

Card Not Present Fraud on the Rise

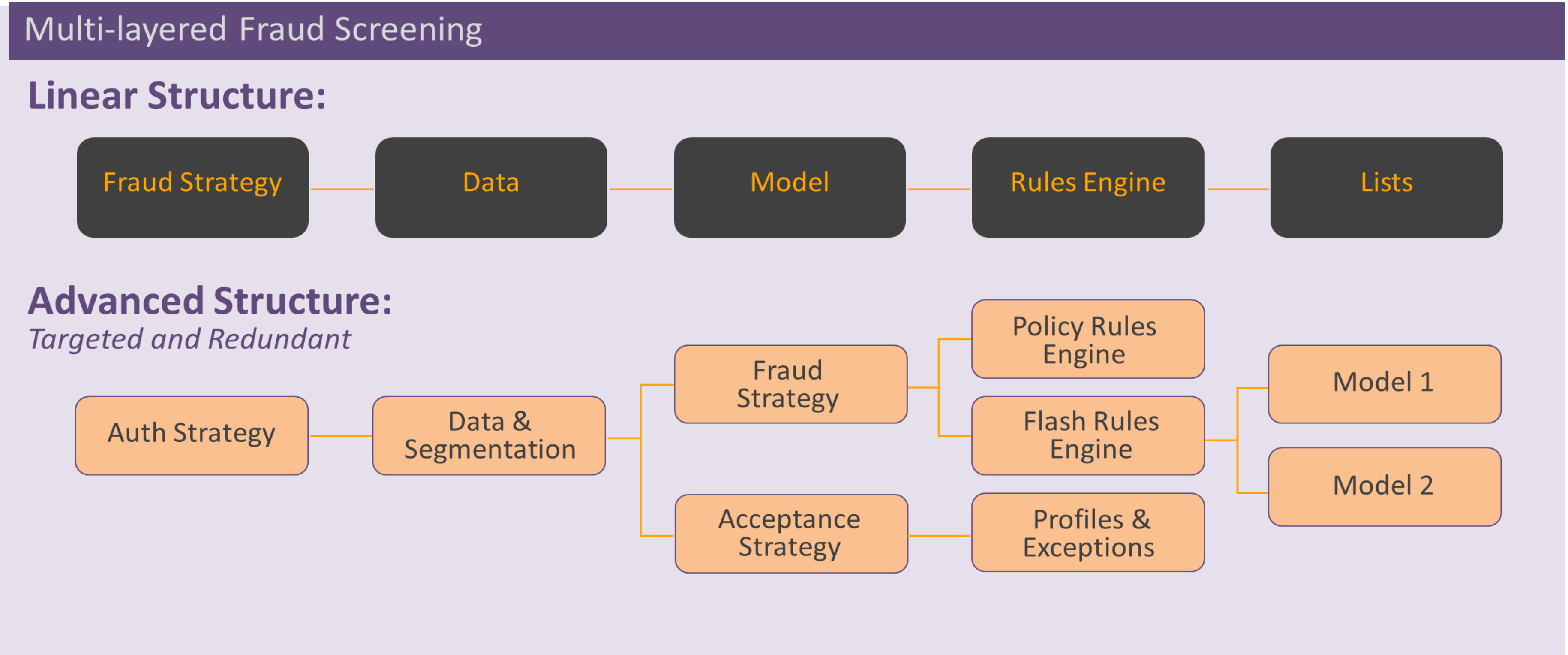
Online card fraud to rise from $4 billion to $7.2 billion by 2020



Dollars Source: Aite Group

© 2017 Jack Henry & Associates, Inc

# Evolution of Fraud Screening



## Multi-layered Fraud Screening

### Linear Structure:

Fraud Strategy — Data — Model — Rules Engine — Lists

### Advanced Structure:

*Targeted and Redundant*

Auth Strategy

Data & Segmentation

Fraud Strategy

Acceptance Strategy

Policy Rules Engine

Flash Rules Engine

Profiles & Exceptions

Model 1

Model 2

SOURCE: MasterCard: “New Ways to Fight Fraud”; Feb 2016

# Use or Fuse Multiple Risk Scores

## Risk Model Integration Best Practices

Option 1

### Let the Best Score Win!

This method assigns scoring rules based on the performance of the individual score ignoring score overlap.

Option 2

### Score Booster!

This method involves adding a score(s) to existing scoring rules to filter additional false positives.

Option 3

### Targeted!

This approach takes advantage of opportunities left with existing scores and strategies by leveraging a specialized score or monitoring service to address specific segments such as international activity, AFD, or secure code.

Option 4

### Integrated!

Leverages the value provided by multiple scores to develop a new set of strategies. This can be accomplished by integrating scores below the threshold used in current rule sets.

SOURCE: MasterCard's Jeff Muschick presentation at 2016 ICBA National Convention: "New Ways to Fight Payment Fraud"

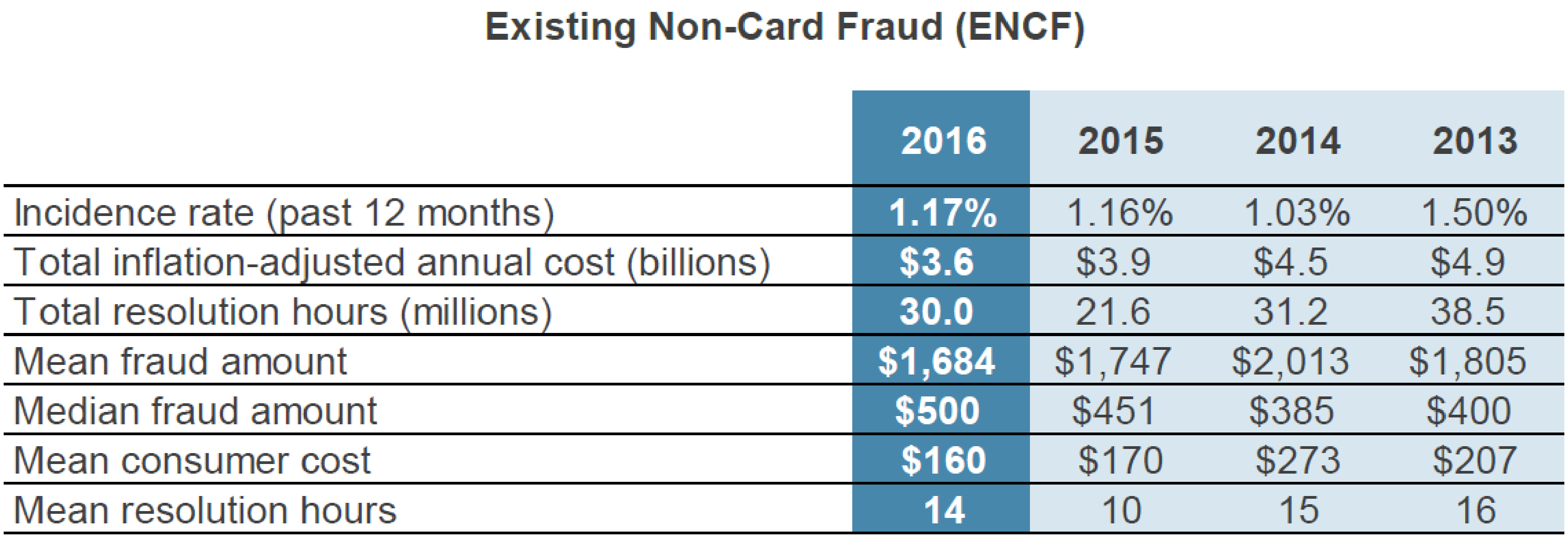
# What to do next…

- **Empower consumers in the fight** with mobile card controls, alert, & no-friction balance access.
- **Ensure your authorization engine has both an acceptance layer and a fraud layer**, to strike a better balance between fraud control and cardholder UX.
- **Use data outside of what is provided by new account applicants to confirm their identities**, e.g., voter registration, property records, social media footprint (avoid SSN-only authentication).

SOURCE: Javelin Strategy & Research; 2016 Identity Fraud: Fraud Hits An Inflection Point; February 2016

© 2017 Jack Henry & Associates, Inc.

# Existing Non-Card Fraud shifts to e-commerce accounts

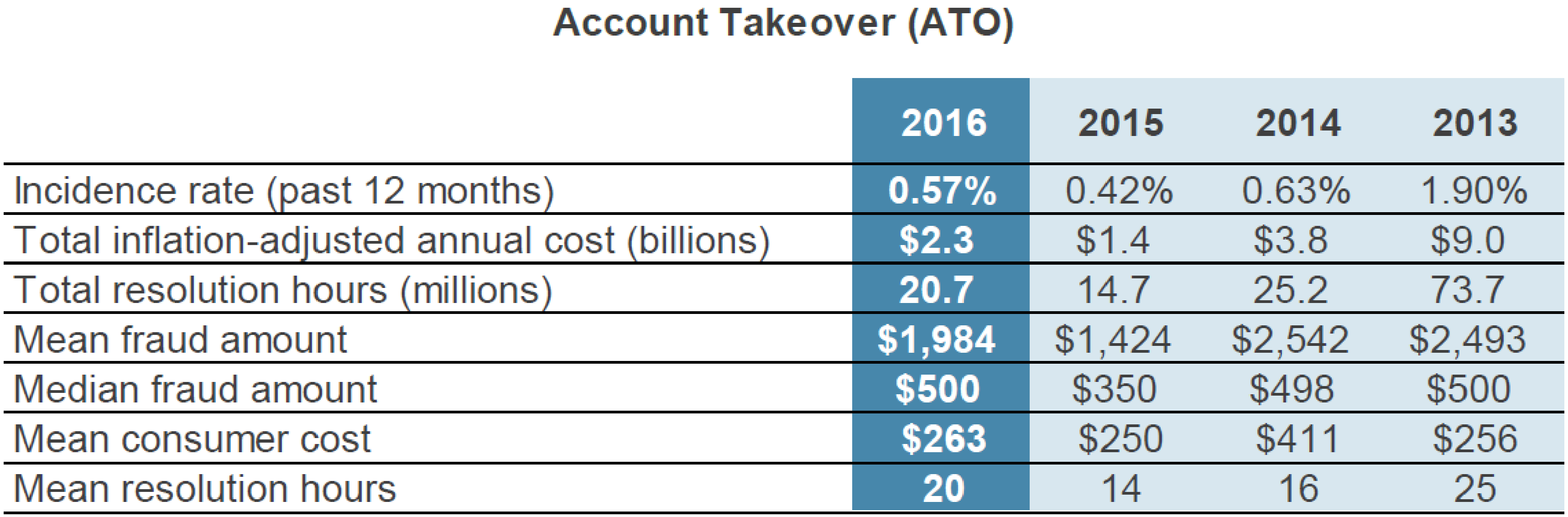


## Existing Non-Card Fraud (ENCF)

| | 2016 | 2015 | 2014 | 2013 |
|---|---|---|---|---|
| Incidence rate (past 12 months) | **1.17%** | 1.16% | 1.03% | 1.50% |
| Total inflation-adjusted annual cost (billions) | **$3.6** | $3.9 | $4.5 | $4.9 |
| Total resolution hours (millions) | **30.0** | 21.6 | 31.2 | 38.5 |
| Mean fraud amount | **$1,684** | $1,747 | $2,013 | $1,805 |
| Median fraud amount | **$500** | $451 | $385 | $400 |
| Mean consumer cost | **$160** | $170 | $273 | $207 |
| Mean resolution hours | **14** | 10 | 15 | 16 |

Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

# Account Takeover (ATO) Fraud costs spike up

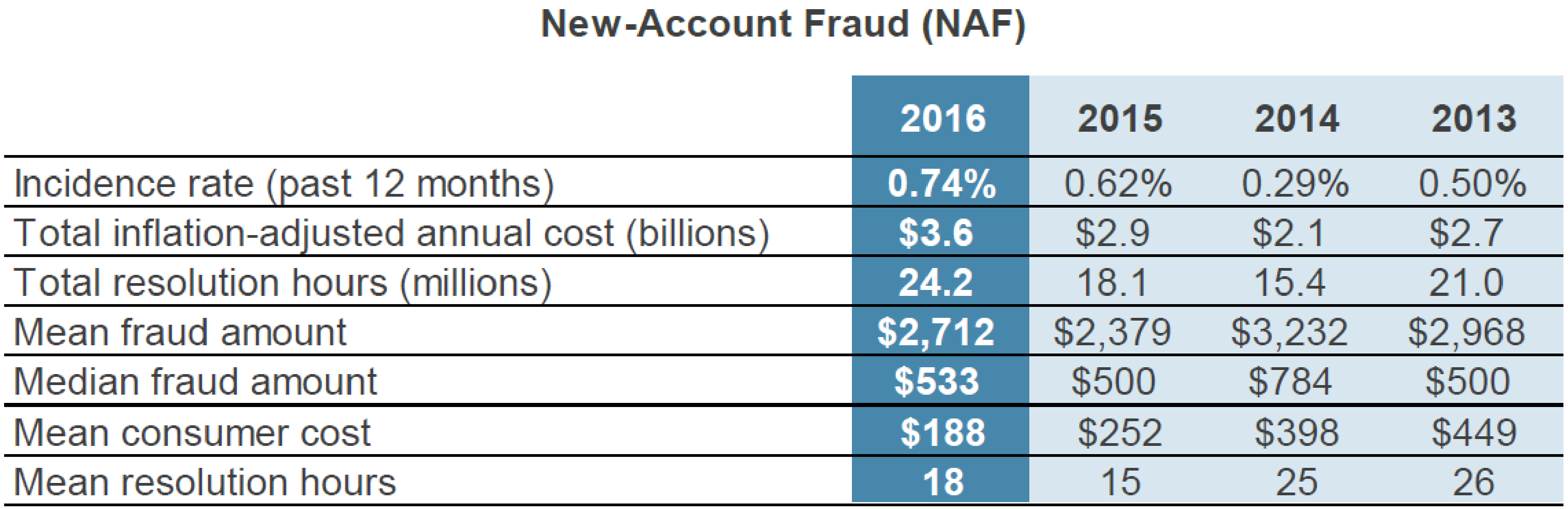


## Account Takeover (ATO)

| | 2016 | 2015 | 2014 | 2013 |
|---|---|---|---|---|
| Incidence rate (past 12 months) | **0.57%** | 0.42% | 0.63% | 1.90% |
| Total inflation-adjusted annual cost (billions) | **$2.3** | $1.4 | $3.8 | $9.0 |
| Total resolution hours (millions) | **20.7** | 14.7 | 25.2 | 73.7 |
| Mean fraud amount | **$1,984** | $1,424 | $2,542 | $2,493 |
| Median fraud amount | **$500** | $350 | $498 | $500 |
| Mean consumer cost | **$263** | $250 | $411 | $256 |
| Mean resolution hours | **20** | 14 | 16 | 25 |

Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

# New-Account Fraud (NAF)



## New-Account Fraud (NAF)

| | 2016 | 2015 | 2014 | 2013 |
|---|---|---|---|---|
| Incidence rate (past 12 months) | **0.74%** | 0.62% | 0.29% | 0.50% |
| Total inflation-adjusted annual cost (billions) | **$3.6** | $2.9 | $2.1 | $2.7 |
| Total resolution hours (millions) | **24.2** | 18.1 | 15.4 | 21.0 |
| Mean fraud amount | **$2,712** | $2,379 | $3,232 | $2,968 |
| Median fraud amount | **$533** | $500 | $784 | $500 |
| Mean consumer cost | **$188** | $252 | $398 | $449 |
| Mean resolution hours | **18** | 15 | 25 | 26 |

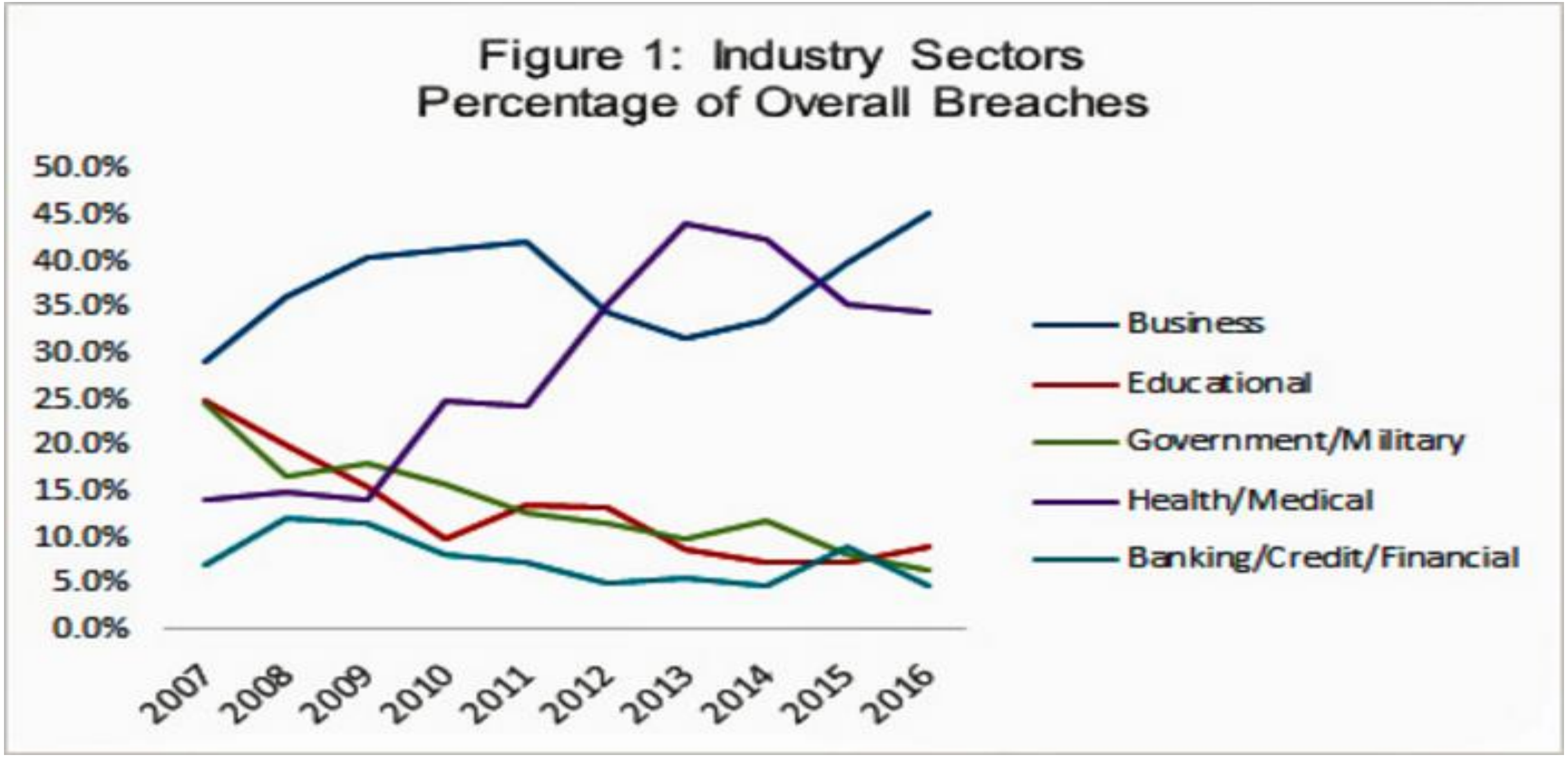
Source: *2017 Identity Fraud Study*, Javelin Strategy & Research

# Data Breach Trendss

- While U.S. data breaches hit an all-time high of 1,093 in 2016, breaches involving financial organizations dropped to 4.8% of all breaches (from 9% in 2015).
  - All-time high may be result of better breach reporting by states
  - Businesses and medical organizations are by far the biggest victims of U.S. data breaches.
- Hacking/skimming/phishing attacks were the most common method of data breach incidents
  - CEO spear phishing related to tax filings (400% surge)

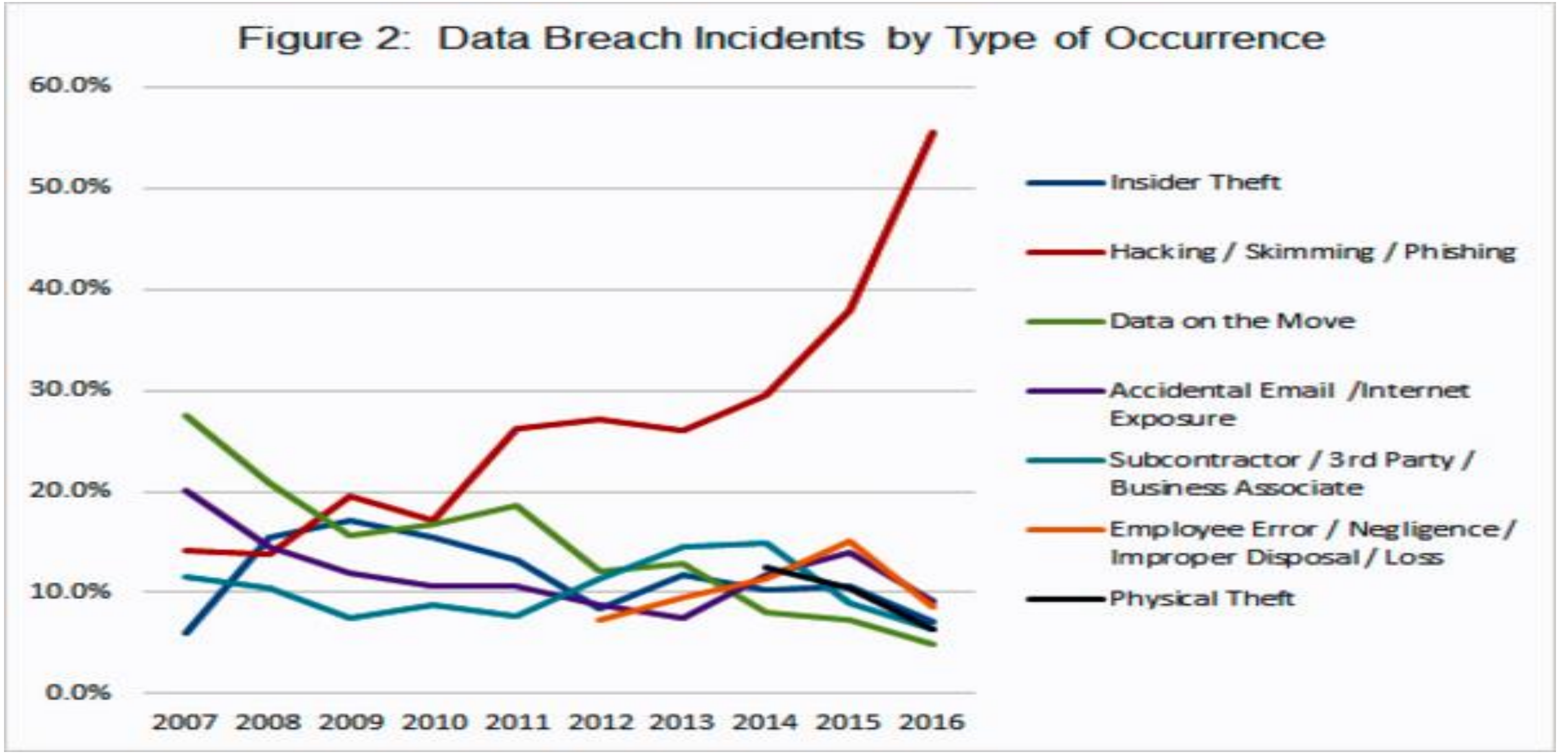
SOURCE: ITRC Data Breach Reports 2016; www.idtheftcenter.org;

# Bank Share of U.S. Breaches Drops



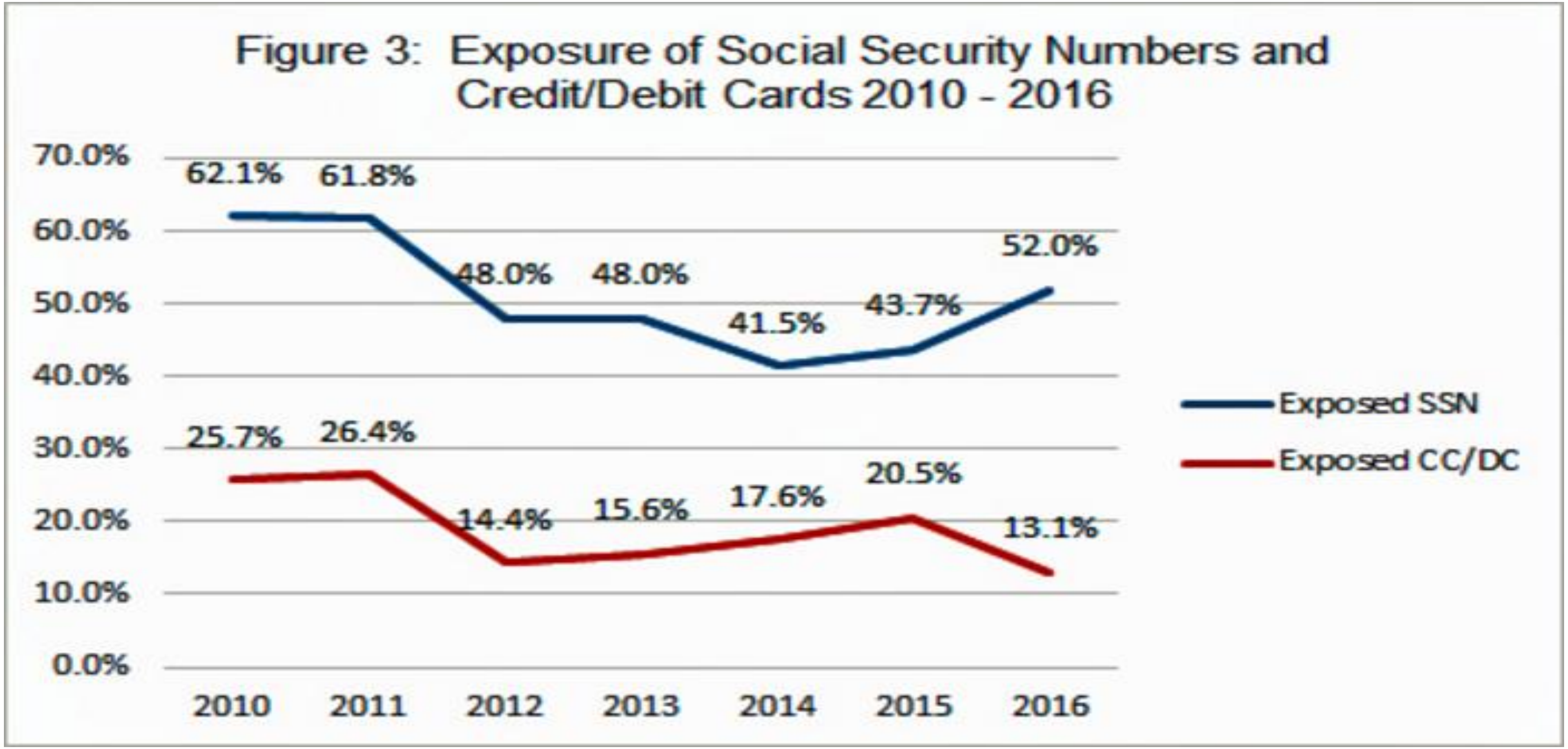
SOURCE: ITRC Data Breach Reports 2016; www.idtheftcenter.org;

# Hacking/Skimming/Phishing Skyrockets



SOURCE: ITRC Data Breach Reports 2016; www.idtheftcenter.org;

# Compromised SSNs & Cards



SOURCE: ITRC Data Breach Reports 2016; www.idtheftcenter.org;

# Compromised Cards Tick Back Up in 2016

**SSN Records Breached Decline Steeply After Record-Setting 2015**

| | | 2015 | 2016 |
|---|---|---|---|
| **Cards** | # of breaches | 160 | 143 |
| | # of records | .8M | → **7.5M** |
| **SSNs** | # of breaches | 338 | → 568 |
| | # of records | 164M | → **19.7M** |

SOURCE: ITRC Data Breach Reports 2015 and 2016; www.idtheftcenter.org;

# Recommendations: Fighting Payments Fraud

- Verification of PII alone is insufficient
  - Applications for new credit card, personal loan, checking
- Leverage customer behavior in and across channels to better identify account takeover
- Anticipate ATO and NAF fraud post-Equifax breach
- Treat fallback transactions with suspicion
- Encourage consumer use of mobile wallets

SOURCE: Javelin 2017 Identity Fraud Study

# Recommendations: Fighting Payments Fraud, cont'd

- Offer CNP transaction alerts to thwart cluster of fraudulent transactions in real-time
- Strong authentication for financial accounts
  - Don't rely on validation of personal information only
  - Still relying on challenge questions from credit bureau?
- Offer customers free or discounted access to ID protection services

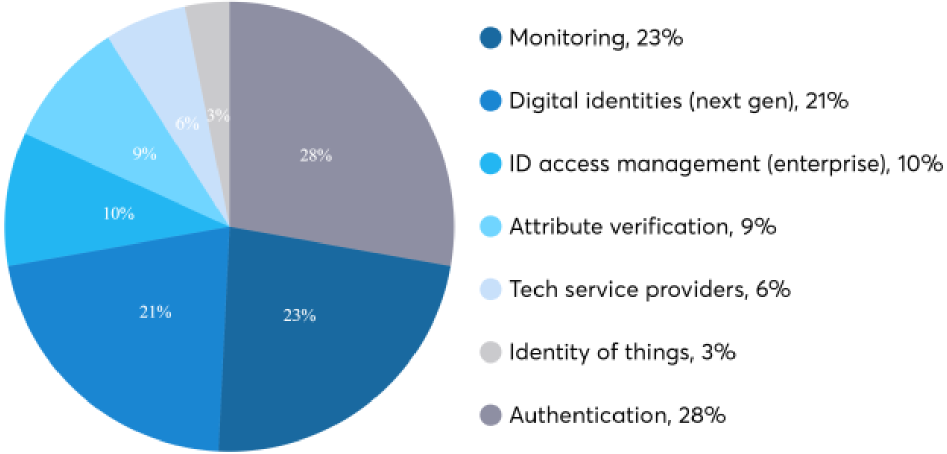
SOURCE: Javelin 2017 Identity Fraud Study

# One ID: The Road to Killing User IDs Passwords?

- FIS & Equifax's **OnlyID**
- Gives consumer one set of credentials
  - a combination of biometrics, behavior analytics, and ID info
- Identifies consumer wherever he/she shops or banks online

**A whole new industry**

An estimated 187 startups offer digital identity services. Most offer partial solutions to a multifaceted problem

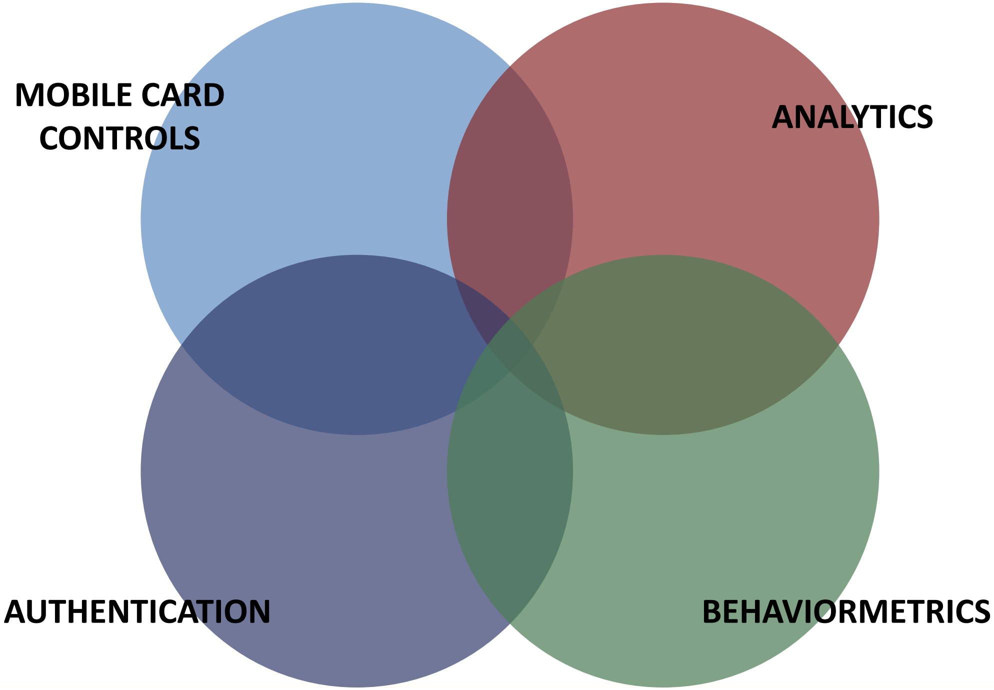


Source: Pascal Bouvier, "The Identity Startup Landscape," finiculture.com, Feb. 10, 2017

SOURCE: www.paymentssource.com; "Heavyweight vendors enter digital ID fray for retailers, banks"; By Penny Crosman; August 23 2017

# Holistic Approach: Fighting CNP Fraud

DRIVING DOWN CNP FRAUD WILL REQUIRE A COMPREHENSIVE STRATEGY



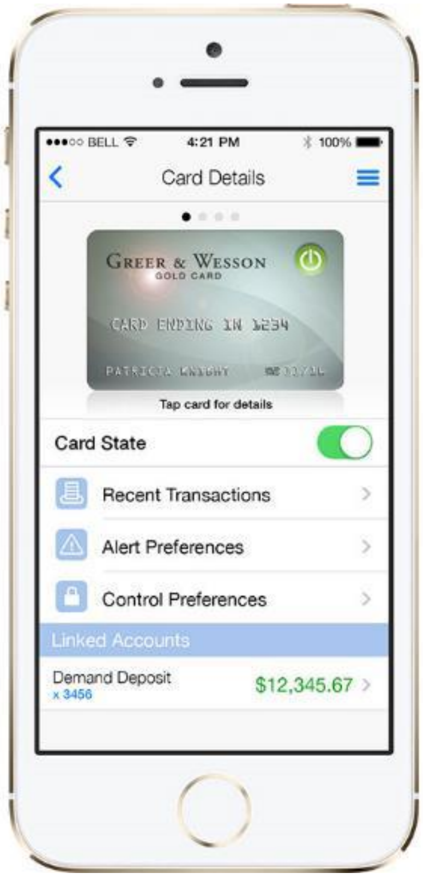
MOBILE CARD CONTROLS

ANALYTICS

AUTHENTICATION

BEHAVIORMETRICS

SOURCE: Javelin Strategy & Research; "Fixing CNP Fraud: Solutions for a Pre- and Post-EMV U.S. Market; October 2014



●●●○○ BELL 4:21 PM 100%

Card Details

GREER & WESSON
GOLD CARD
CARD ENDING IN 1234
PATRICIA KNIGHT

Tap card for details

Card State ●

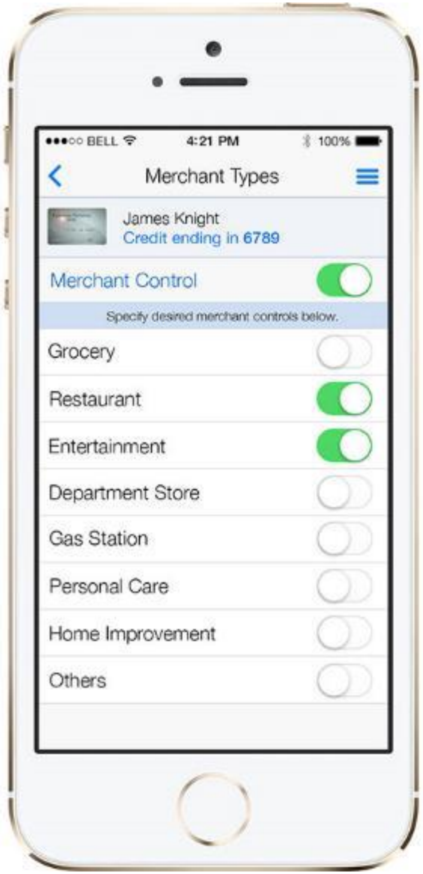
Recent Transactions ›

Alert Preferences ›

Control Preferences ›

Linked Accounts

Demand Deposit
x 3456 $12,345.67 ›



●●●○○ BELL 4:21 PM 100%

Merchant Types

James Knight
Credit ending in 6789

Merchant Control ●

Specify desired merchant controls below.

Grocery ○

Restaurant ●

Entertainment ●

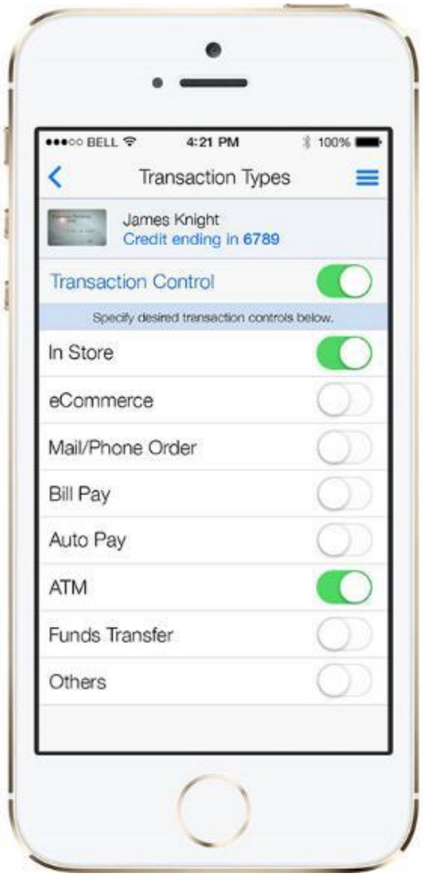
Department Store ○

Gas Station ○

Personal Care ○

Home Improvement ○

Others ○



●●●○○ BELL 4:21 PM 100%

Transaction Types

James Knight
Credit ending in 6789

Transaction Control ●

Specify desired transaction controls below.

In Store ●

eCommerce ○

Mail/Phone Order ○

Bill Pay ○

Auto Pay ○

ATM ●

Funds Transfer ○

Others ○

ondot

# Cardholder-Defined Card Controls

- Toggle card on/off
- Where can card be used
  - Geolocation, e.g., local-only, regional, international?
  - Acceptable merchant categories
- When can card be used
  - Time of day/night:  weekdays, weekends, etc.
- What kinds of transactions are allowed
  - In-store, e-commerce, mail/phone order, billpay, auto-pay (card on file), ATM, funds transfers, etc.

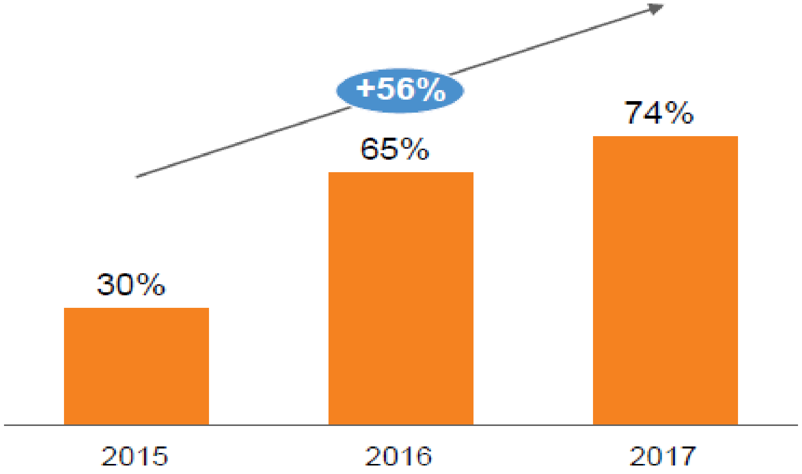
SOURCE: Javelin Strategy & Research: “FIXING CNP FRAUD: Solutions for a Pre- and Post-EMV U.S. Market”

© 2017 Jack Henry & Associates, Inc.

# Leverage Mobile Wallet Biometrics/Tokenization

## Percentage of issuers with cards eligible to be loaded onto mobile wallets

By year, as of January[1]



## Apple Pay remains the most popular option

| Mobile wallet | Percentage of issuers[2] |
|---|---|
| Apple Pay | 74% |
| Samsung Pay | 55% |
| Android Pay | 51% |
| Other wallet | 26% |

Note: The Study focuses on instances of "mobile payment" where the smartphone is used as the payment device at a physical POS

[1] 2015 and 2016 data is from the 2016 *Debit Issuer Study*

[2] Does not sum to 100% since many issuers offer more than one wallet

©2017 Jack Henry & Associates, Inc.

# The Internet of Things Moves In

The 2014 U.S. edition of Deloitte's Global Mobile Consumer Survey reveals that smartphone owners overindexed in their desire for Internet of Things (IoT) solutions for the home and car.

### Would find value in smart **HOME** solutions

| | |
|---|---|
| smartphone owners | 65% |
| all consumers | 55% |
| consumers willing to pay for smart home solutions | 71% |

### Would find value in connected **CAR** solutions

| | |
|---|---|
| smartphone owners | 72% |
| all consumers | 63% |
| consumers willing to pay for connected car solutions | 60% |

## SMART HOME
% of most valued technologies

**Home Control** 47%
lights, heating and burglar alarms controlled by smartphone

**Home Monitoring** 40%
in-home camera footage viewed and controlled by smartphone

**Entertainment** 20%
entertainment systems display social media postings

**Appliance Control** 18%
sensors in appliances send notifications to smartphone

**Landscape Control** 9%
landscape systems measure plant moisture, watering only when necessary

## CONNECTED CAR
% of most valued technologies

**Traffic/Weather** 40%
real-time traffic and weather updates displayed on in-car screens

**Navigation** 39%
mapping and route optimization

**Maintenance** 28%
automated diagnosis and tracking of vehicle's systems

**Access** 23%
remotely lock and track vehicle via Internet-connected device

**Entertainment** 18%
music streaming to in-car entertainment system

**Fuel Tracking** 18%
fuel efficiency tracking

**Automation** 10%
driverless operation

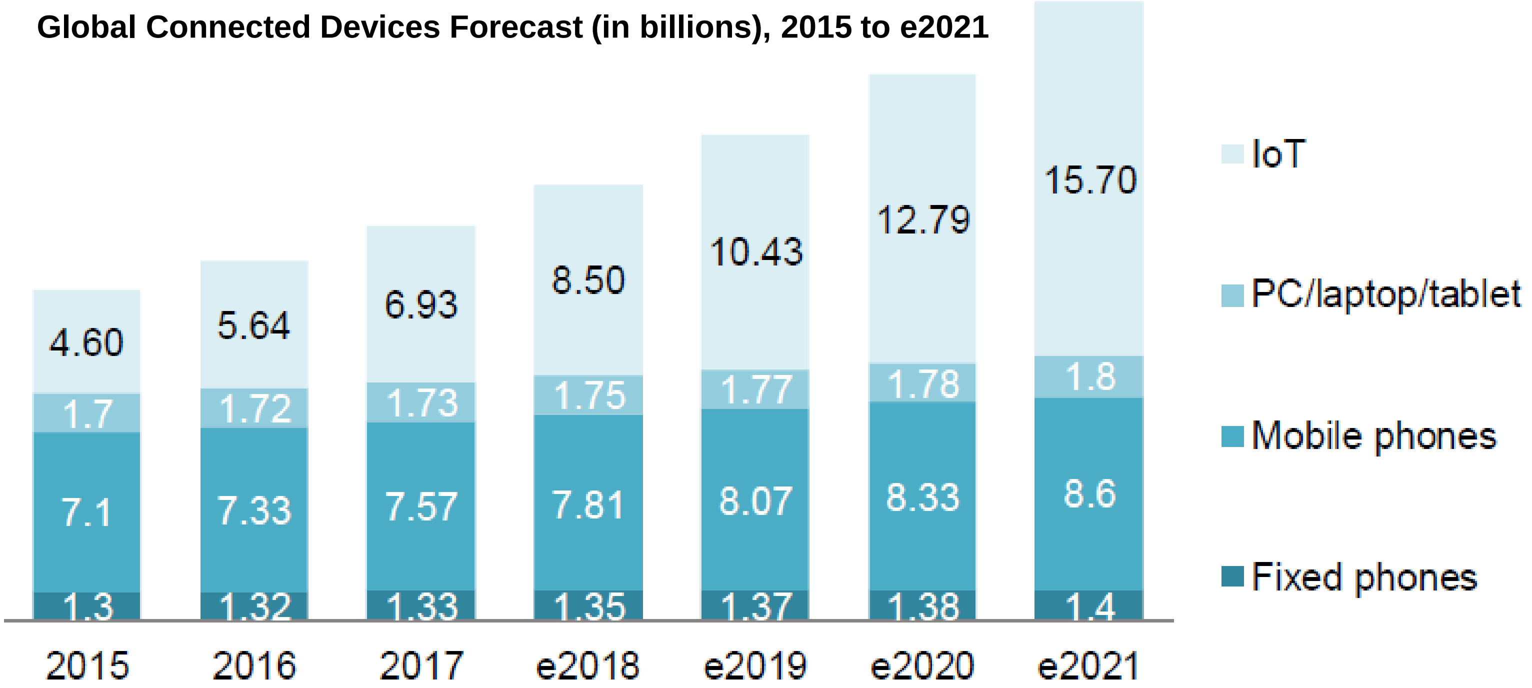
While the least valued connected technology is the self-driving car, **60%** of all consumers would be willing to pay for one.

### Younger Generations (18-24)

**17%** Compared to other consumers surveyed, the youngest generation valued landscape control the most. Do they not want to do their chores?

**16%** Surprisingly, the youngest generation is also the age group most interested in self-driving cars. Would they rather text than get behind the wheel?

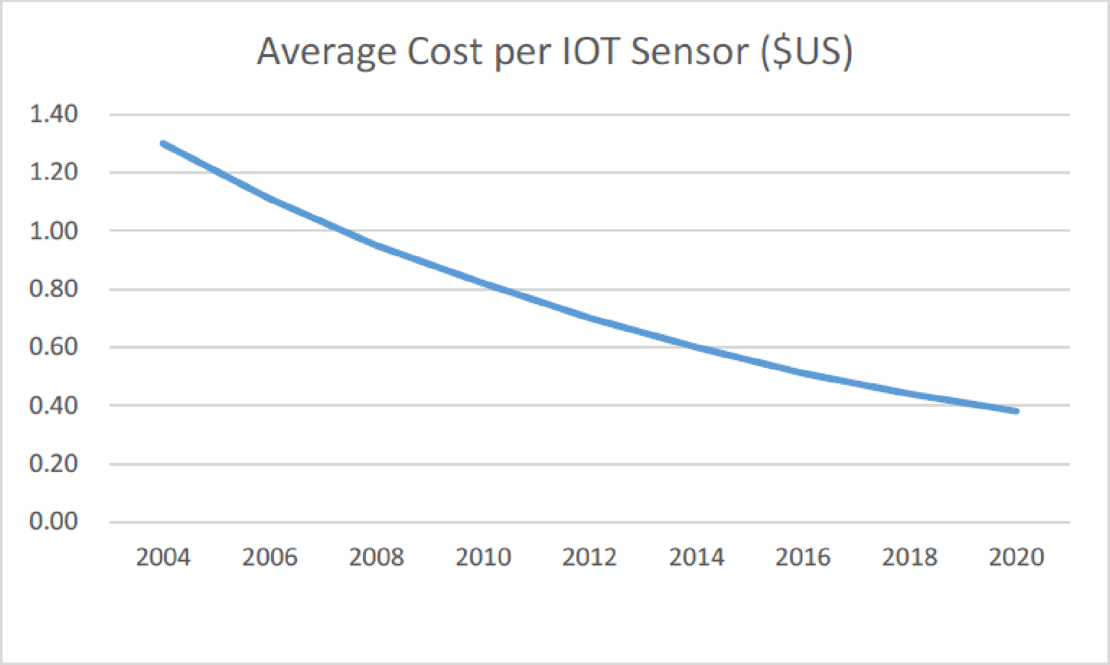
# Global Connected Devices



SOURCE: Ericsson Mobility Report 2016, Aite Group analysis

SOURCE: Aite Group; “The Internet of Things: An Information Explosion”; May 2017

# Sensors: Costs Go Down; Deployments Go Up



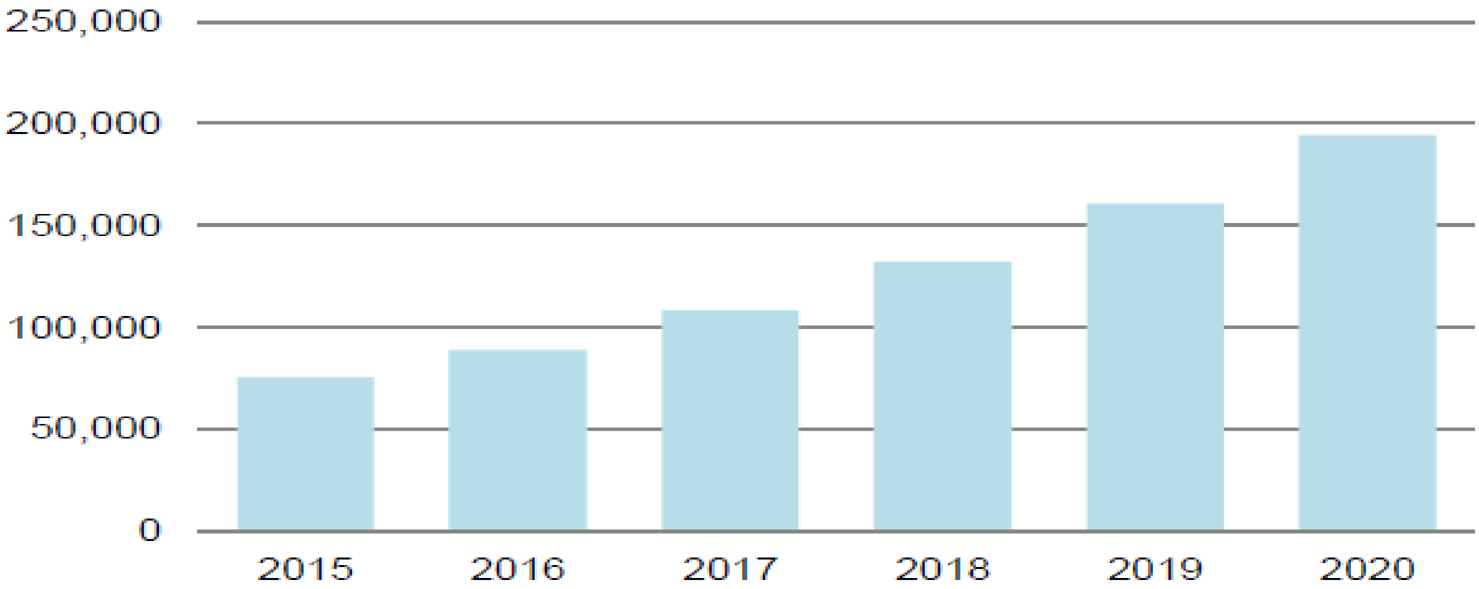
*Source: Goldman Sachs, BI Intelligence*

SOURCE: Aite Group; "The Internet of Things: An Information Explosion"; May 2017

# Internet Data Volumes Grow 21% Annually

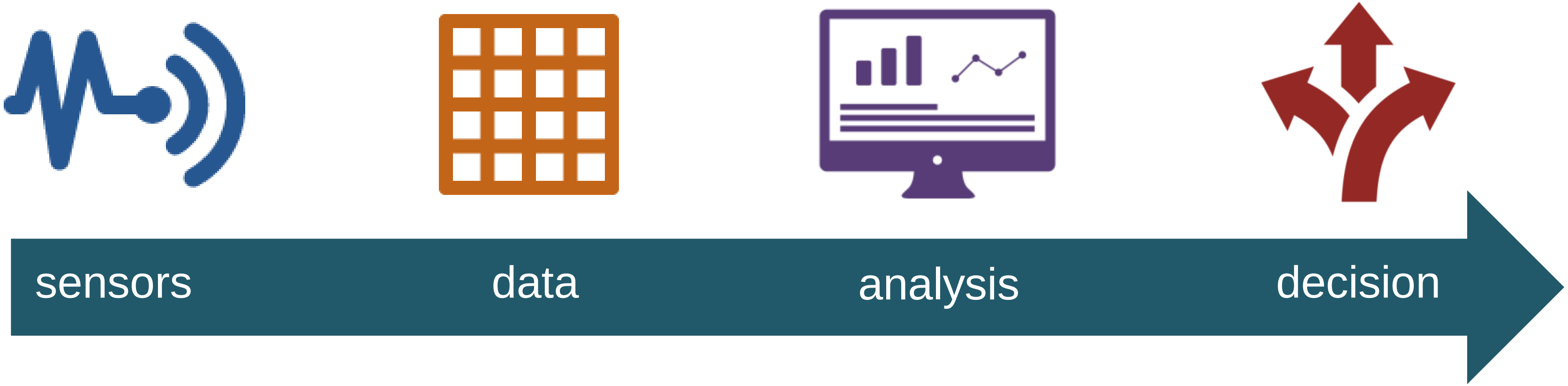
Global IP Data Growth, 2015 to 2020 (In exabytes)

SOURCE: Cisco Visual Networking Index



SOURCE: Aite Group; “The Internet of Things: An Information Explosion”; May 2017

# Internet of Things (IoT), Data, Analytics & Decisioning



# IoT Impacts on Payments and Security

- More payments for lower amounts
  - Shift from periodic (monthly) to real-time, on-demand, a la carte payments…will challenge authorization capacity
  - Machine-to-Machine (M2M) payments between machine-based accounts or value stores?
- Unsecured IoT devices amplify power/scale of botnets
- As payments automate, “top of wallet” card becomes defacto “only card” in wallet

# Lee Wetherington

## lwetherington@jackhenry.com

### http://discover.profitstars.com/leewetherington

@leewetherington

Linked in

http://www.linkedin.com/in/leewetherington

jack henry
& ASSOCIATES INC.