ONLINE/MOBILE IDENTITY MANAGEMENT AND RISK ASSESSMENT

Jay Johns – Global Partner Manager

IACA

May 2017

About Us

FOUNDED: 2004

HEADQUARTERS: Portland, Oregon

EMPLOYEES: 150

CUSTOMERS: 600+, 6 Continents, 18 Time Zones

BRANDS WE PROTECT: 1,500+

SOLUTIONS: Fraud Prevention and Authentication

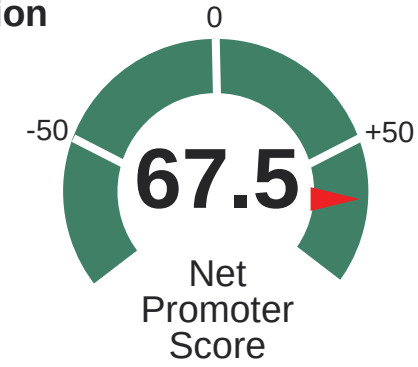
COMMUNITY: 3,500 Fraud Professionals

TRANSACTIONS MONITORED: 35B and climbing

TRANSACTIONS PER DAY: 20+ million

SYSTEM DOWNTIME 3+ YEARS: 0 min

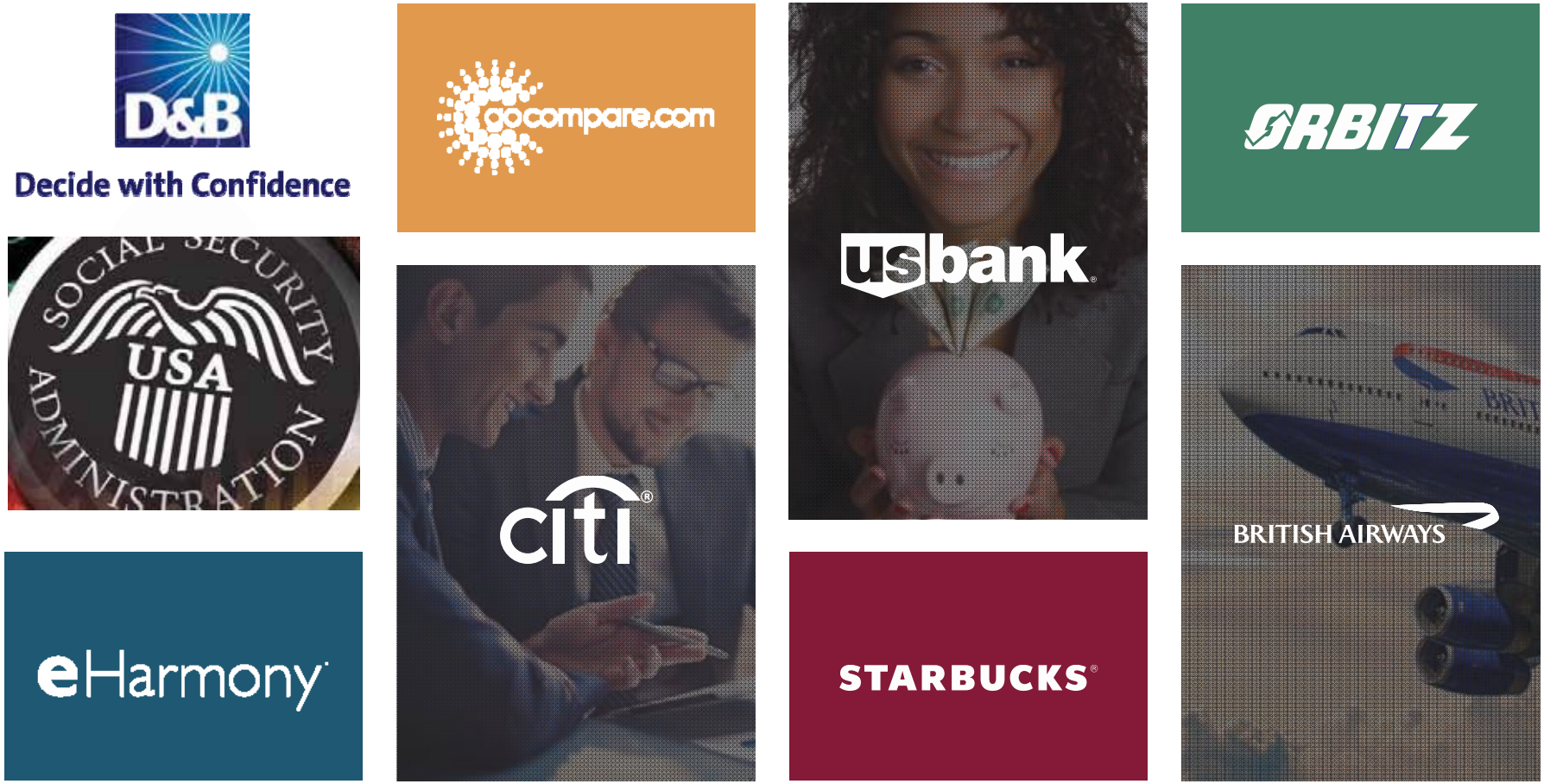
98% customer retention and industry-leading customer satisfaction



9 U.S. patents for device recognition, detection, and authentication

iovation…

…. unites your fraud, security, and business teams with a common platform for customer authentication and fraud prevention while ensuring an outstanding customer experience.


D&B
Decide with Confidence
gocompare.com
usbank
ORBITZ
SOCIAL SECURITY ADMINISTRATION
USA
citi
BRITISH AIRWAYS
eHarmony
STARBUCKS

WHERE DOES ONLINE/MOBILE FRAUD BEGIN?

CREDIT CARD THEFT

KrebsonSecurity
In-depth security news and investigation

BLOG ADVERTISING ABOUT THE AUTHOR

02 Breach at Sabre Corp.'s Hospitality Unit

MAY 17

Breaches involving major players in the hospitality industry continue to pile up. Today, travel industry giant **Sabre Corp.** disclosed what could be a significant breach of payment and customer data tied to bookings processed through a reservations system that serves more than 32,000 hotels and other lodging establishments.

In a quarterly filing with the **U.S. Securities and Exchange Commission** (SEC) today, Southlake, Texas-based Sabre said it was "investigating an incident of unauthorized access to payment information contained in a subset of hotel reservations processed through our Hospitality

Sabre

WHERE DOES ONLINE/MOBILE FRAUD BEGIN?

IDENTITY THEFT

News > California News

Officials: Foreign government may be behind Anthem data breach

1

By THE ASSOCIATED PRESS |
January 6, 2017 at 4:47 pm

SACRAMENTO — A foreign government may have been behind a cyber breach of health insurance company Anthem that compromised the records of more than 78 million consumers, investigators said Friday. They declined to identify the hackers or the foreign government.

Social Security numbers, birthdates and employment details of customers were accessed

WHERE DOES ONLINE/MOBILE FRAUD BEGIN?

MALWARE

SecurityIntelligence
Analysis and Insight for Information Security Professionals

NEWS 35 TOPICS INDUSTRIES X-FORCE RESEARCH MEDIA EVENTS & WEBINARS

Home > News >

NEWS January 30, 2017 @ 1:00 PM

Newly Discovered Banking Malware Creates Fresh Threat to Users

By Mark Samuels

Researchers have found another threat that users have to worry about. Security firm Cyren recently discovered a wave of

TRENDING NEWS

IBM Guardium Takes the Overall Leadership Position in the First Database Security Leadership Compass by KuppingerCole
Read More

The Health Care Data Breach: A Tale of Big Expenses and Cheap Sales
Read More

WHERE DOES ONLINE/MOBILE FRAUD BEGIN?

SKIMMING

Card skimmer found at Manitowoc gas station

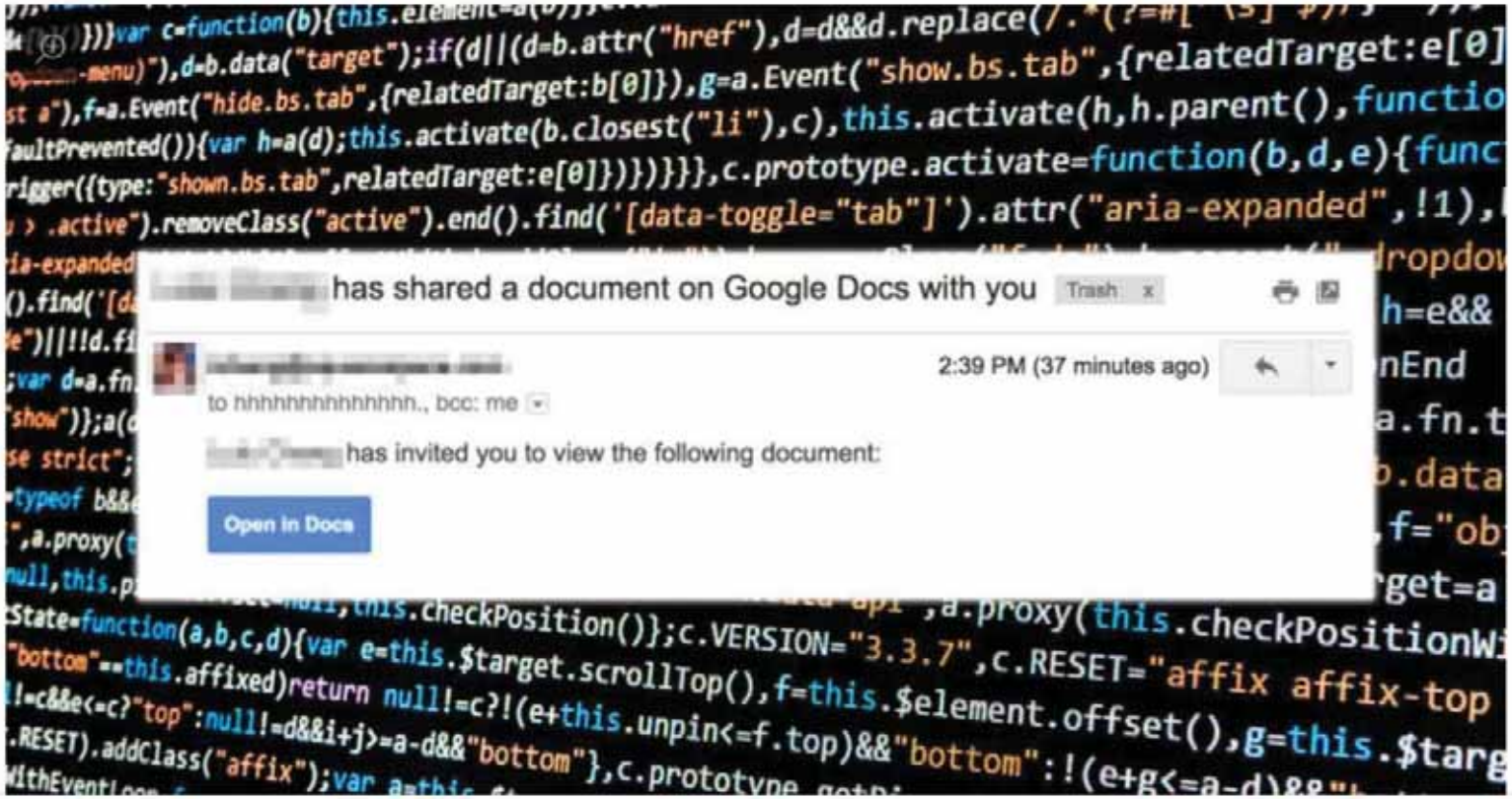
by FOX 11 News |

ADVERTISEMENT

TRENDING

WHERE DOES ONLINE/MOBILE FRAUD BEGIN?

PHISHING



HOW HACKERS SELL DATA

DARK WEB

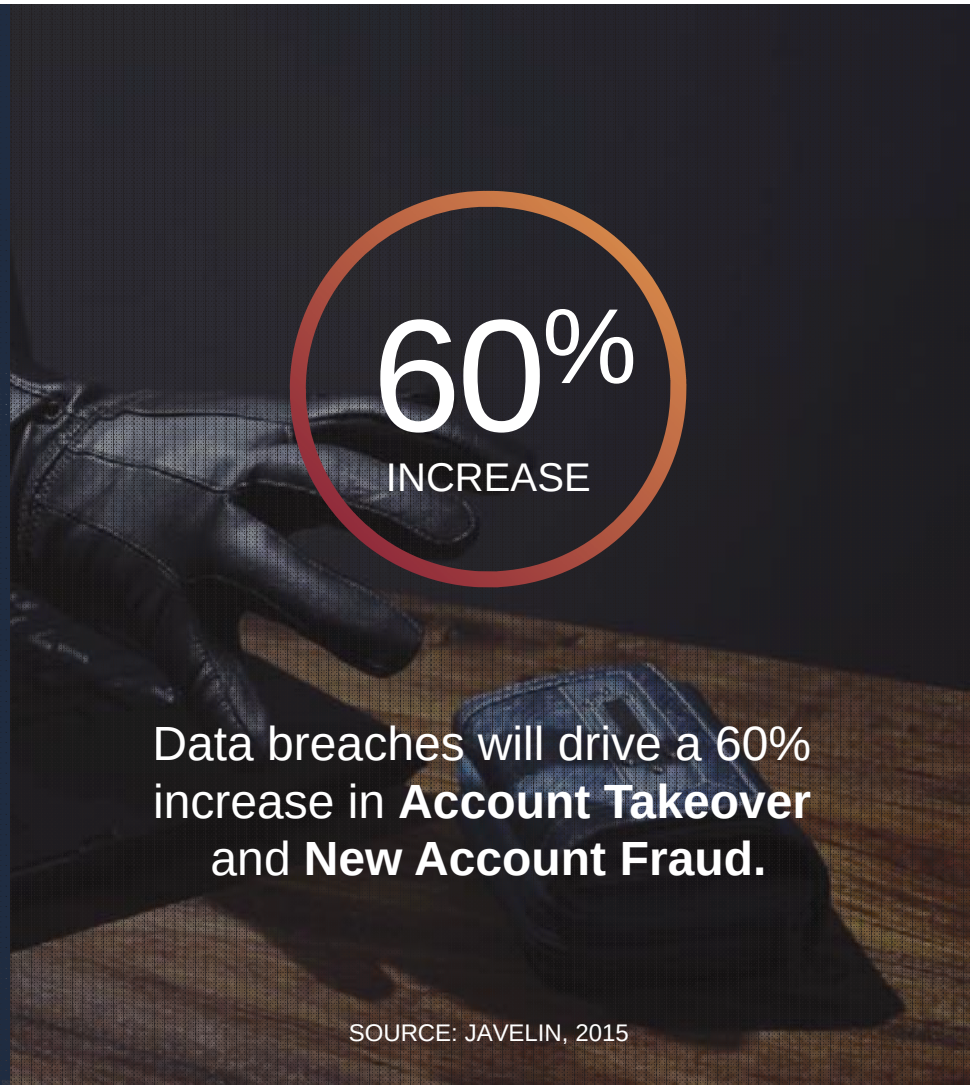
HOW HACKERS SELL DATA

DARK WEB

DATA BREACHES

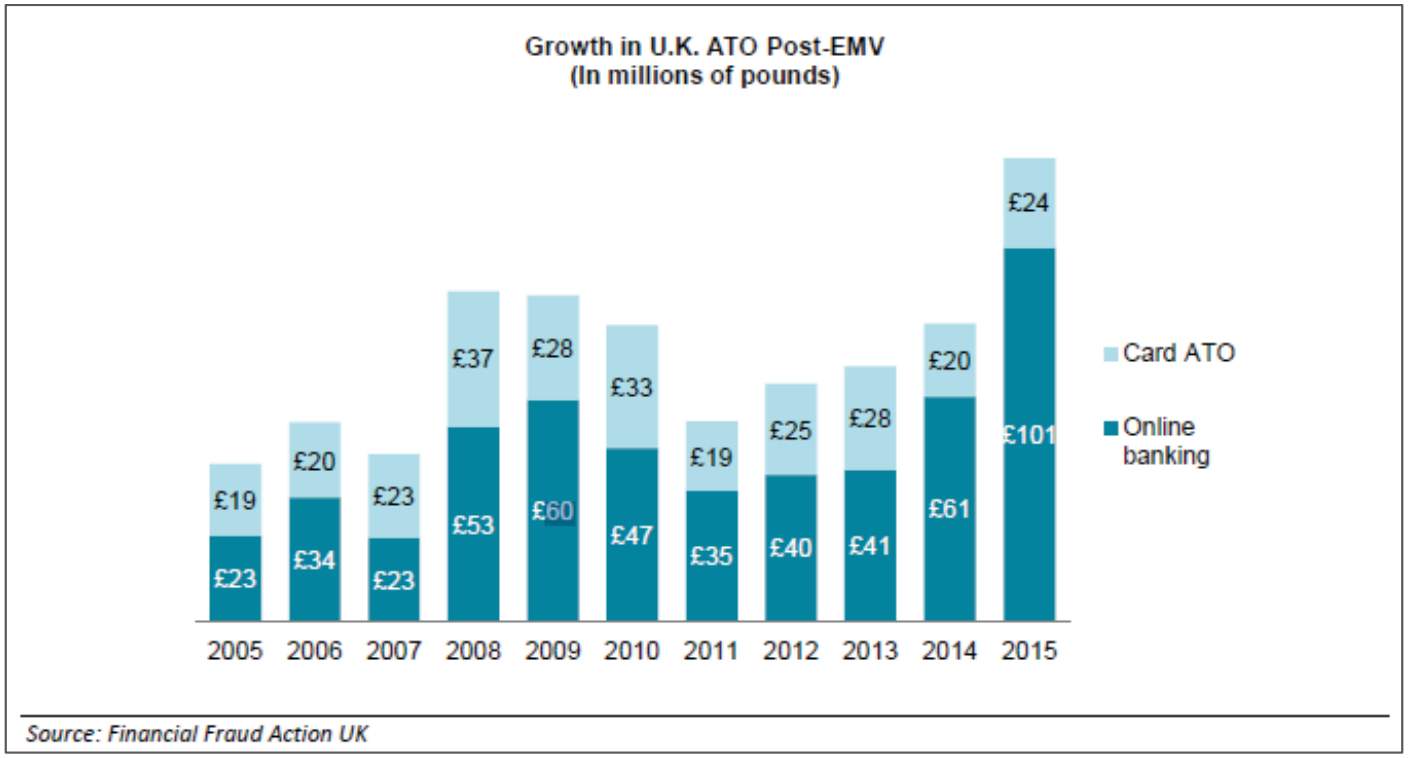
$5B in 2014

$8B in 2018



GROWTH OF ONLINE FRAUD

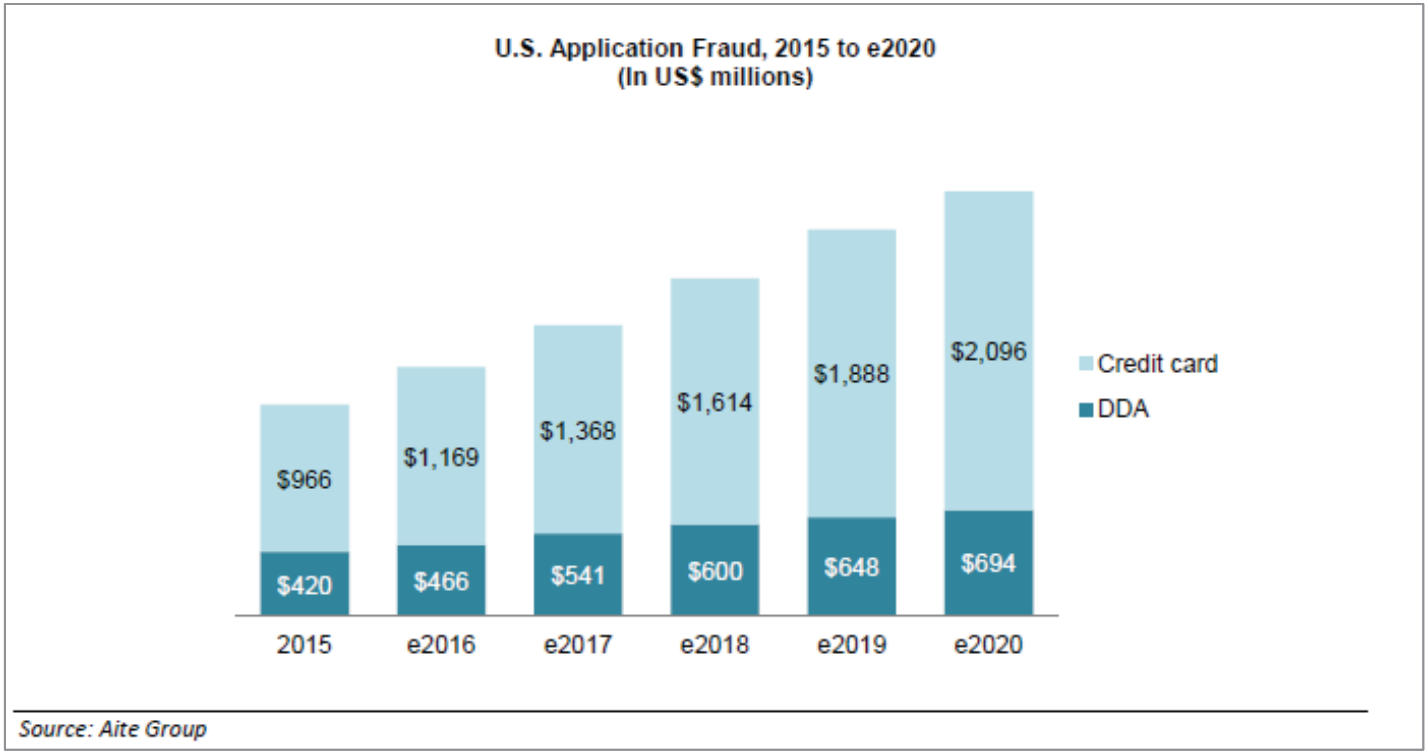
ACCOUNT TAKEOVERS



Source: Financial Fraud Action UK

GROWTH OF ONLINE FRAUD

APPLICATION FRAUD



Source: Aite Group

PROJECTED IMPACTS IN THE U.S.

CNP FRAUD

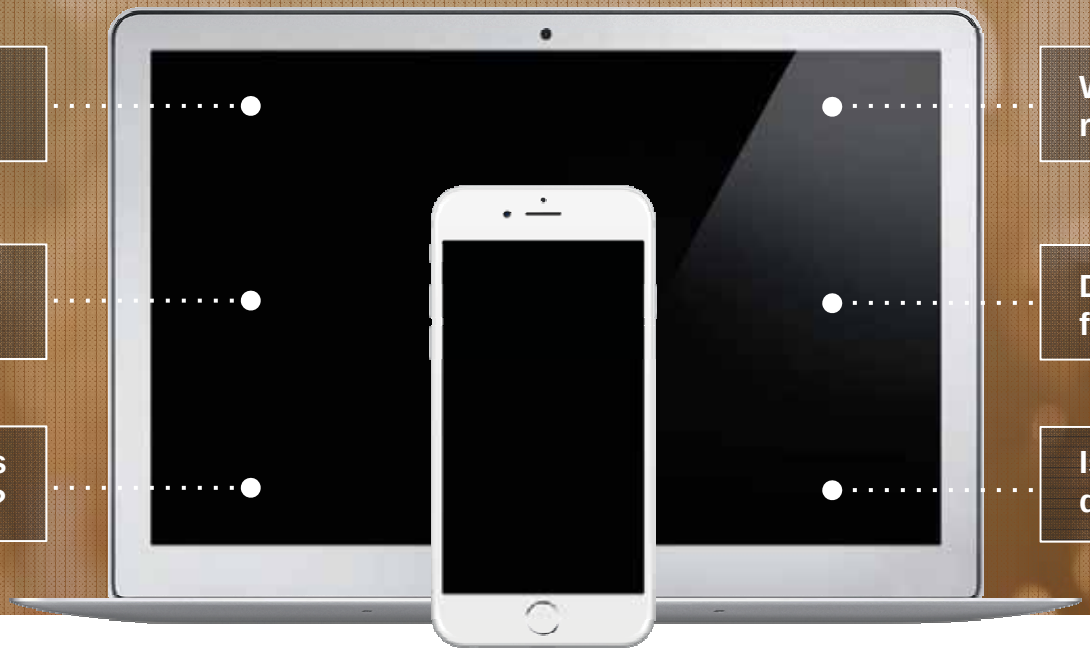
A potentially disastrous increase in Card Not Present fraud

CNP fraud is **projected to see a 80% increase** over the next 4+ years

Source Aite Group
"EMV: Issuance Trajectory and Impact on Account Takeover and CNP," May 2015

The Power of Device Intelligence.

Every device tells a story.



- Is device authorized for this account?
- Where is device located?
- How many accounts has device accessed?
- What other devices are related to this device?
- Does device have a fraud history?
- Is device hiding from detection?

DEVICE RECOGNTION

HUNDREDS OF DEVICE ATTRIBUTES COLLECTED

Web Device Print

- MD5 Hash of the full font list
- Random sample of 15 fonts
- Flash SharedObjects not writable
- Flash socket 843 based ip (real IP)
- Boolean indicator: flash took longer than expected to execute
- Accepted Char Sets in HTTP header
- Flash 3-part version (16.0.0)
- Flash 4-part version (16.0.0.305)
- List of browser plugins
- JavaScript screen resolution
- Simbar toolbar GUID from HTTP hdr
- Timezone offset in minutes
- ... and more

iOS SDK

- WiFi (or Bluetooth) MAC Address
- Network configuration
- iOS Device Model
- Battery level / AC mode
- Device orientation
- File system size
- Physical memory
- OS Name and/or version
- Device advertising UUID
- Kernel version
- iCloud Ubiquity Token
- Application Vendor UUID /name/vers
- Locale language / currency code
- … and more

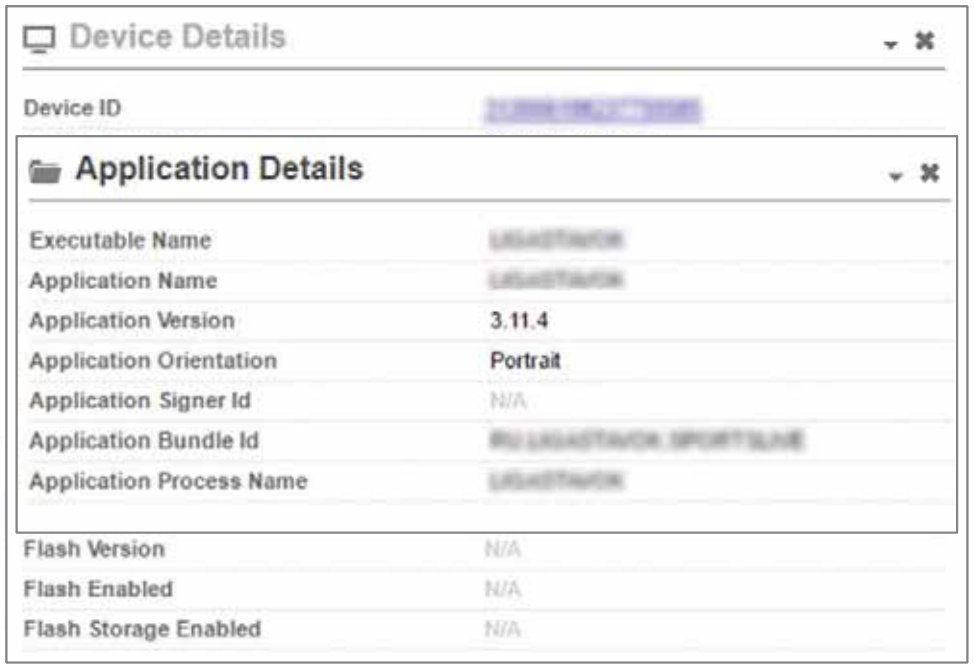
Android SDK

- Model and Device Model
- Build.DEVICE & Build.HARDWARE
- Build.HOST & Build.ID
- Manufacturer
- Build.PRODUCT & Build.TIME
- Network Operator ID & Name
- Sim Operator ID & Country
- Android Build Number (DISPLAY)
- Android Device System Version
- Detected attempt at hiding root detect
- Kernel Version (was AKV)
- Android Locale Country Code
- Desktop Wallpaper Hash
- … and more

Unique adaptive analytics are used to determine the combinations of attributes needed to achieve the most accurate device recognition.

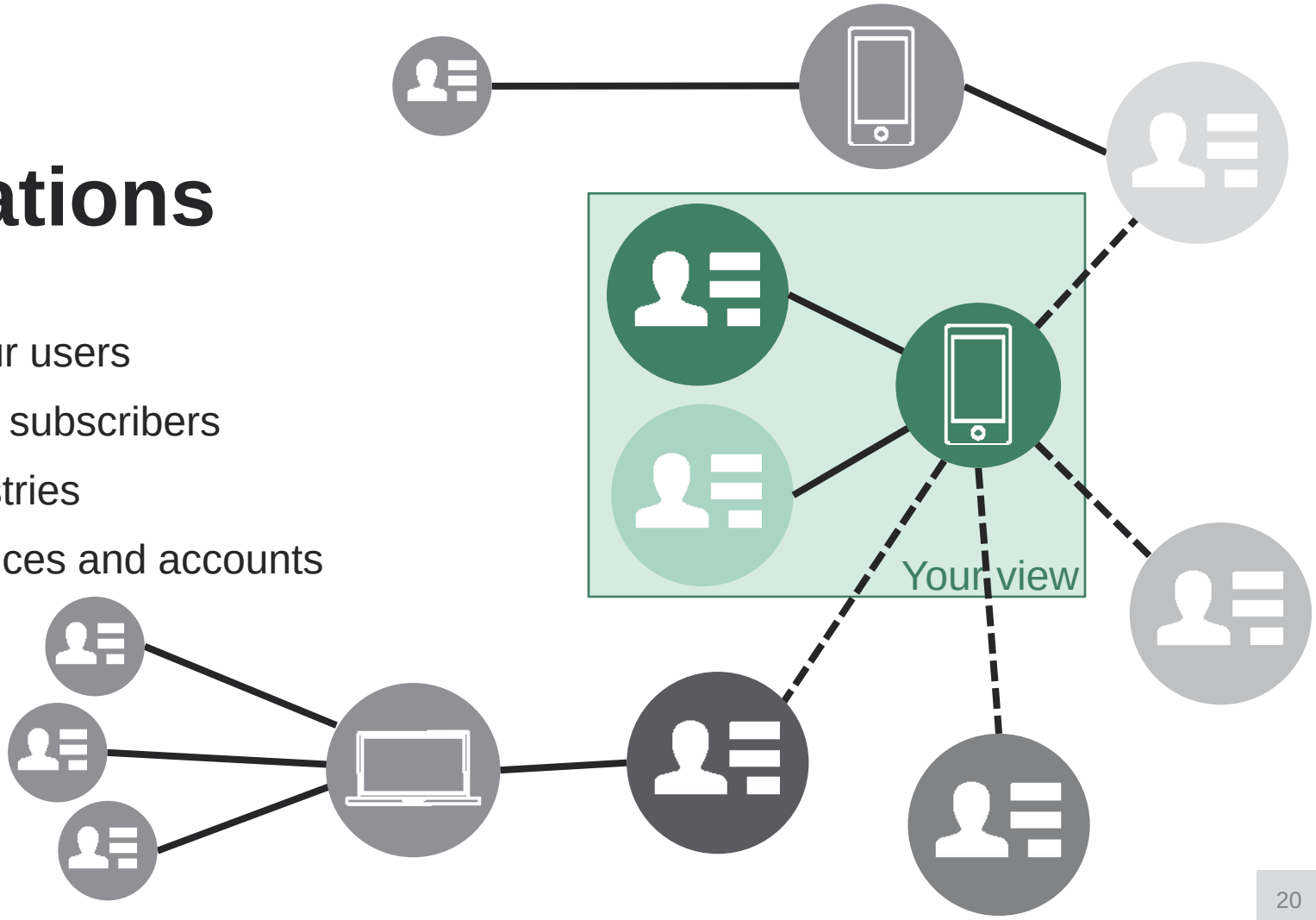
GRANULAR DEVICE AND TRANSACTION DETAILS

RETURNED IN OUR REAL-TIME RESPONSE
AND SEARCHABLE IN THE INTELLIGENCE CENTER



Device Associations

- Between your users
- Across other subscribers
- Across industries
- To other devices and accounts



DETAILED FRAUD REPORTS

UNDERSTAND WHY THE TRANSACTION WAS DENIED

FINANCIAL
- Credit Card Fraud
- ACH/Debit Fraud
- Friendly Chargeback
- Insufficient Funds
- Fraud - Other
- Potential Fraud
- Shipping Fraud
- Counterfeit Money Order
- Click Fraud
- Affiliate Fraud
- First Party Fraud
- Loan Default

MISCONDUCT
- Chat Abuse
- Spam
- Abusive to Support
- Promotion Abuse
- Policy /License Violations
- Customer Harassment
- Inappropriate Content
- Profile Misrepresentation
- Scammer/Solicitation
- Code Hacking
- Arbitrage Betting
- Gold Farming

CHEATING
- Collusion
- Chip Dumping
- All-in Abuse
- Trading Restriction

ID THEFT
- True Identify Theft
- Synthetic Identity Theft
- ID Mining/Phishing
- Account Takeover
- Failed Multi-Factor Authentication

POLICY FRAUD
- Application Fraud – 1st Party
- Application Fraud – 3rd Party
- Claims Fraud – 1st Party
- Claims Fraud – 3rd Party

B2B FINANCIAL
- Business Identify Theft
- Fictitious Business
- Business Takeover
- Dealer Fraud
- Payment Evasion
- Business Misrepresentation

OTHER
- High Risk
- Under or Over Age
- Requested Exclusion

Within 100ms, iovation ...

and returns a transaction result based on factors that you've defined

ALLOW	REVIEW OR CHALLENGE	DENY
Nothing negative was associated with the device	Risk or new device seen, may want to manually review or challenge	Device has history of fraud, other serious risk factors, or violates your policies

PROCESSES TO CONSIDER

Device Reputation/Device Analytics

Process Analytics Tools

Bureau Data

Phone Number Data Bureaus

CVV2

Address Verification

Custom Developed Knowledge Based Authentication

Push ACH

Machine Learning

Maintain internal block lists and cross-channel alerts

BUILDING A STRONG DEFENSE

Build a defense in depth waterfall strategy
Maintain Fraud Manager Position
Develop a toolset that addresses each area of risk individually
Consider constituent user experience
Utilize transparent technologies that doesn’t expose fraud prevention practices
Collaborate with peers
Engage Law Enforcement
Monitor performance of tools
Adjust rules to adapt to emerging threats
Provide strong defenses on high value accounts
Share Online/Mobile threat data with processing personnel
Limit export of Personally Identifiable Information

THANK YOU