# Combating Emerging Payments Fraud

Mike Corbera

revopay

35th Annual SoCal Expo

04.07.16

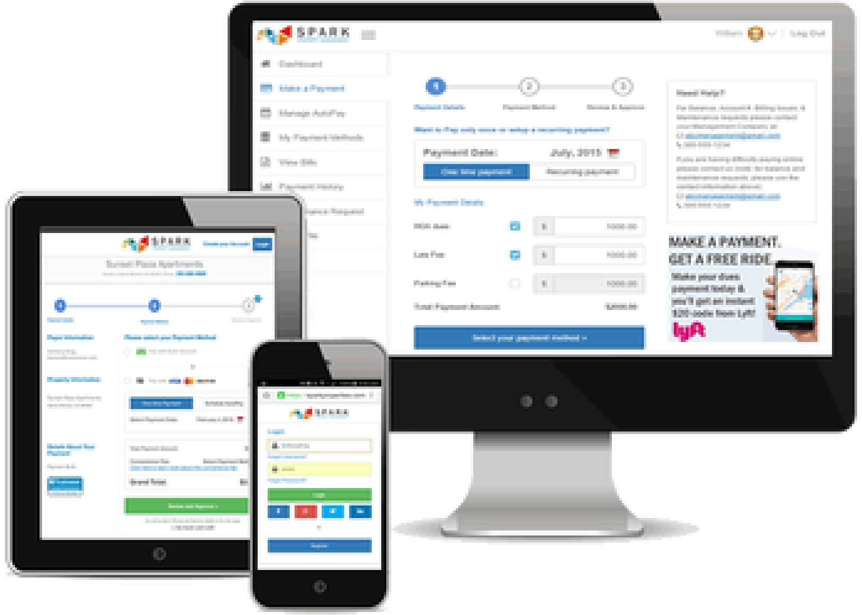
As CEO of RevoPay, Mike Corbera leads strategy, sales, marketing, technology and operations for the company.

A former attorney specializing in the areas of Payments and eCommerce, Mike is a graduate of Vanderbilt Law School and Harvard Business School.

He is licensed to practice law in both Florida and California, home to RevoPay's dual headquarters. He has published several articles about payments and software and is a frequent speaker on the banking and payments circuit.

revopay

- Most Flexible API Tools in the Industry
- Innovative Features That Make the Resident Experience Simple
- Highest Resident Adoption Rates & Resident Rewards



# Payments Fraud

## Overview

- **62%** of companies were targets of payments fraud in 2014
  *2015 AFP Payments Fraud and Control Survey*

- **$32 billion** was the cost of fraud to US Retailers in 2014
  *LexisNexis 2014*

- **$16 billion** was stolen from consumers.
  *2015 Identity Fraud Report, Javelin Strategy & Research*

# Payments Fraud

## Card-Not-Present

### What is CNP?

- Transaction where cardholder doesn’t or can’t physically present card for merchant’s visual examination at time of order
- Interchange rates between CNP and CP transactions differ

- Represents 45% of total U.S. card fraud
  *Aite Group, 2014*

- CNP fraud losses totaled $10 billion in 2014, but they’ll jump to $19 billion in 2018.
  *2015 Data Breach Fraud Impact Report*

# Payments Fraud

## Card-Not-Present

➢ U.S. online and mobile commerce growing at 15% annual rate

*(Aite Group 2014)*

### Online

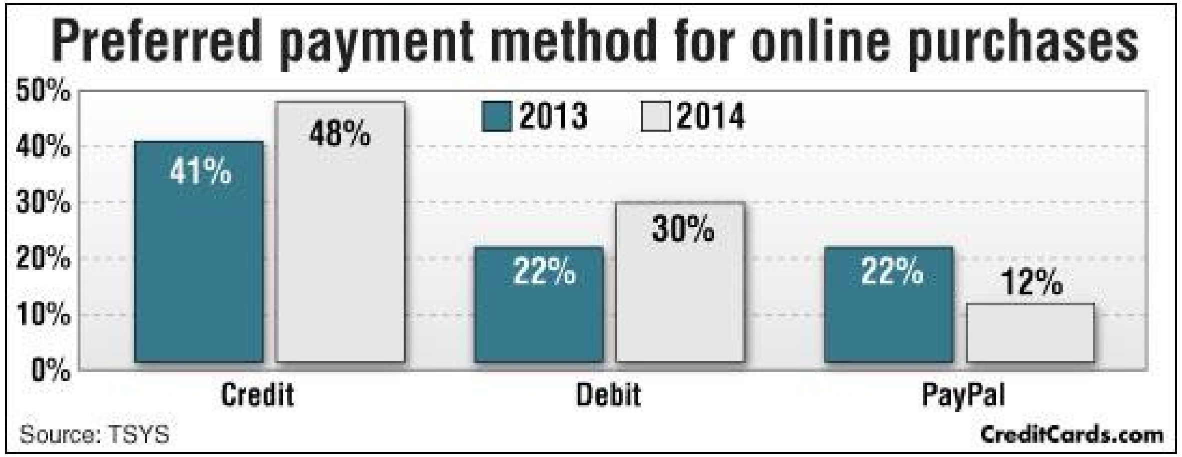
- 55% of merchant fraud cases were from online sales in 2015 (up 31% from 2014)

  *Marketwatch 2015*

### Mobile

- Relatively new payment method - recent surge in popularity
- 14% of U.S. transactions via m-commerce channels in 2014
- 21% of all fraudulent transactions in 2014 were mobile
- Cost of mobile fraud: highest of any channel $3.34 for every dollar

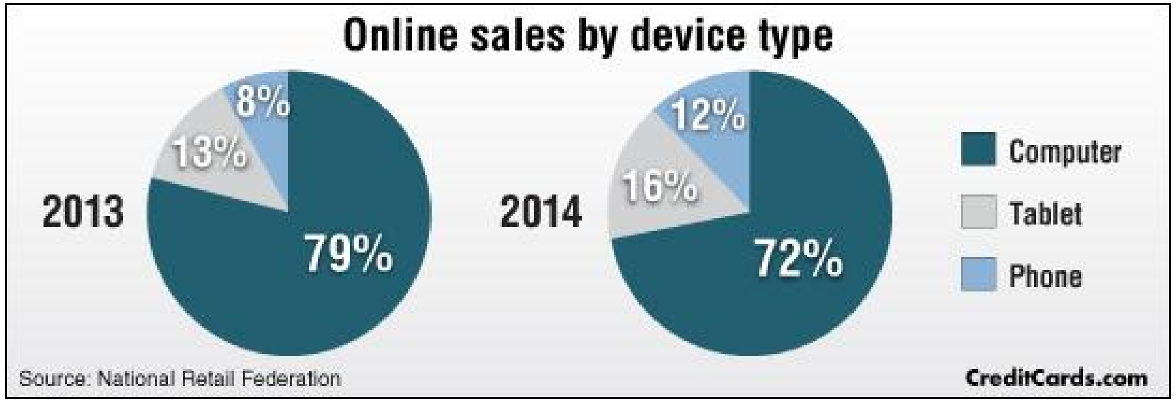
  *LexisNexis 2015*



Preferred payment method for online purchases

Source: TSYS

CreditCards.com



Online sales by device type

Source: National Retail Federation

CreditCards.com

# Payments Fraud
## Current Practices

- 7 out of 10 organizations conduct daily reconciliation of transaction activity
- 40% of companies implementing systems to ensure disaster recovery plans include ability to continue with strong controls and maintain in-office compliance when enacting disaster recovery
- 28% companies restrict company network access for payments to company issued laptops
- 20% restrict network access for payments via mobile devices

*2015 AFP Payments Fraud and Control Survey*

# Effect of Technology on Payments Fraud

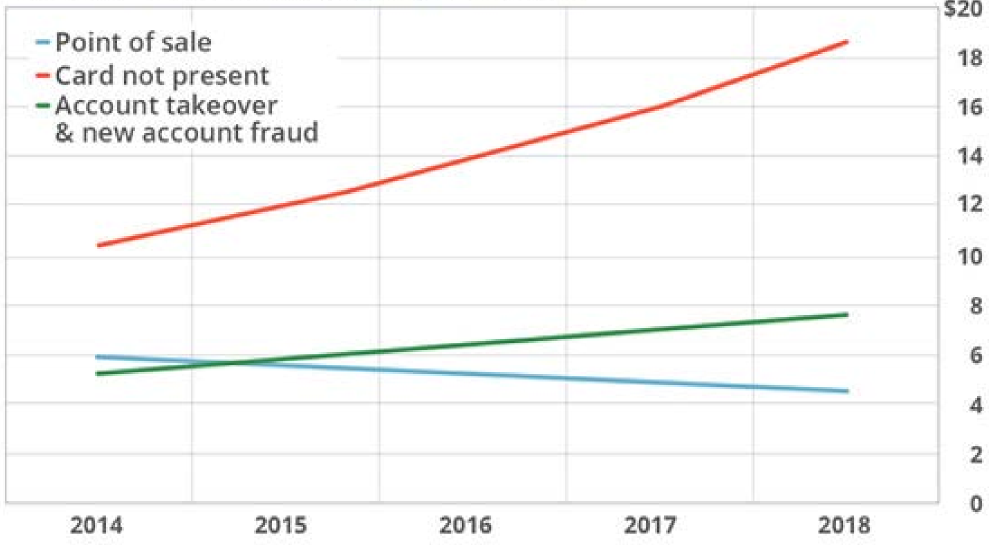
## EMV chip cards

**EMV** - Standard that ensures chip-based payment cards and terminals are compatible around the world

- ➢ Refers to Europay, MasterCard and Visa - developed specifications in 1994

- ● Combination of card number validation via chip and user authentication via PIN offers stronger protection against attacks (Fraudulent use of stolen or lost cards/ counterfeit cards/ skimming/ etc.)
  - o 90% expected increase in CNP fraud
  - o CNP fraud losses totaled $10 billion in 2014, $19 billion projected in 2018 *2015 Data Breach Fraud Impact Report*

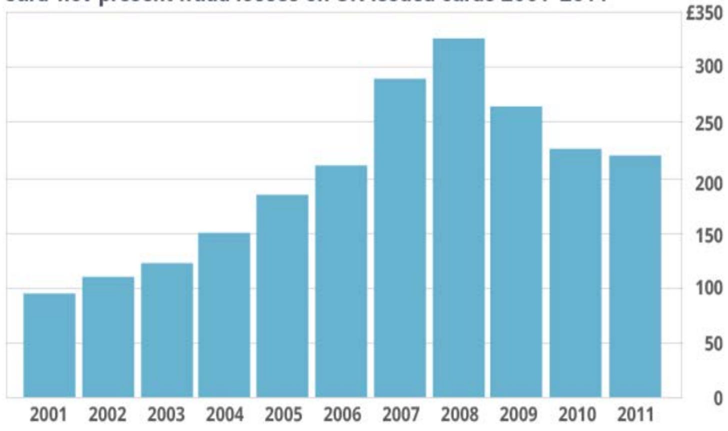
Credit card fraud projections



Source: Javelin Strategy & Research

How fraud shifted online when other countries moved to EMV

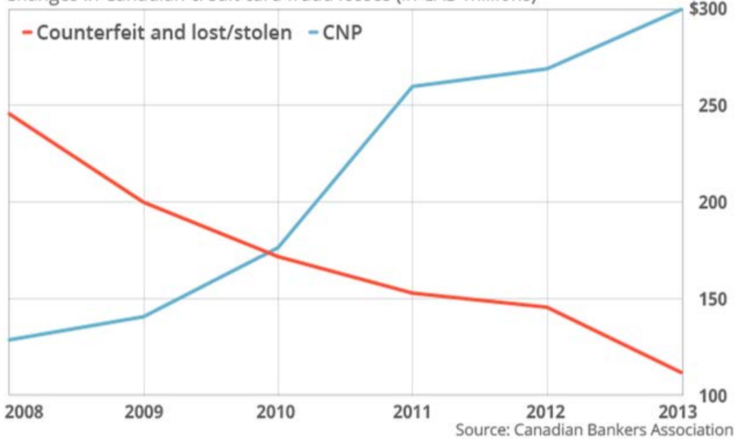
Card-not-present fraud losses on UK-issued cards 2001-2011



Source: Financial Fraud Action UK

Canadian card-not-present (CNP) and point-of-sale (POS) credit card fraud losses

Changes in Canadian credit card fraud losses (in CAD millions)



Source: Canadian Bankers Association

# Technology's Impact on Payments Fraud

## Cloud Systems/ Wi-Fi

Cloud and dark web open Internet to cybercrime in new ways

- ➢ More data exchanged without user awareness
- ➢ Cybercriminals gain easy access to information

### Cloud Systems

- Enable organizations to take advantage of cost savings, flexibility, massive computing power
- Gives cybercriminals anonymity
- Cybercriminals leverage free offerings
- CaaS - cybercrime as a service: ability to purchase products/ services to start life in cybercrime
  - Starter kits, customized malware, packages containing stolen card information

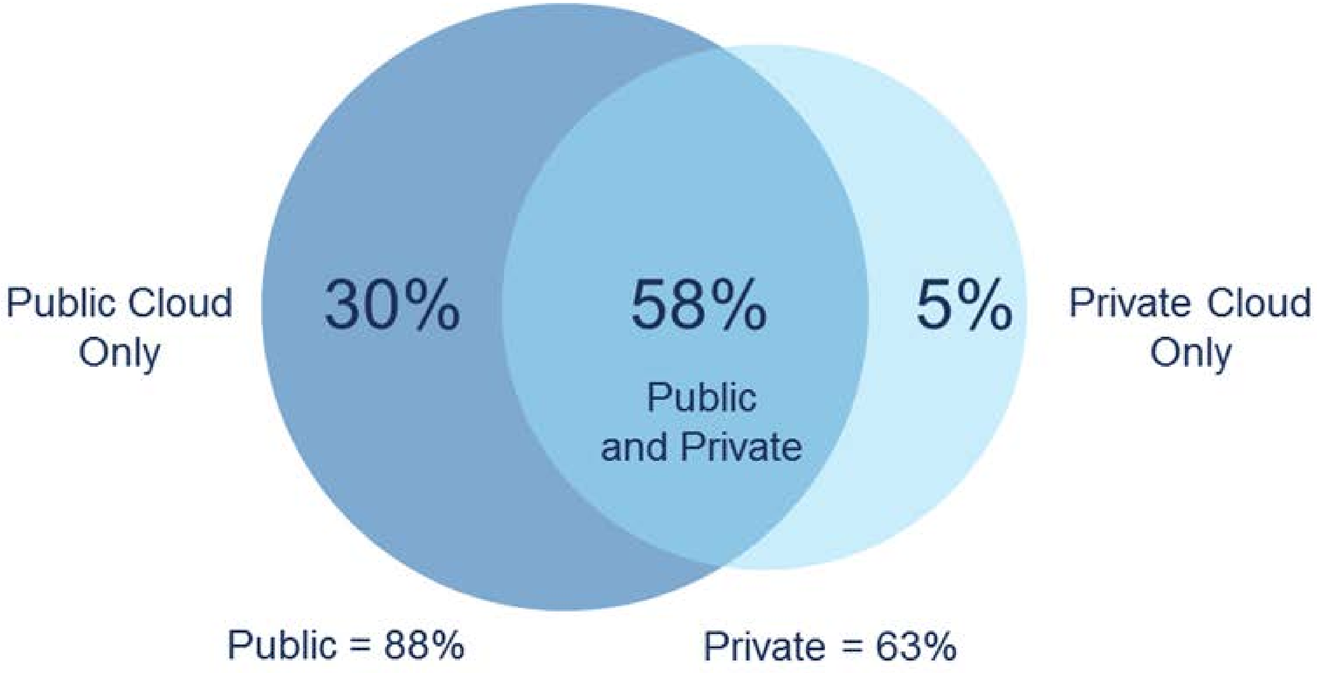
### Wi-Fi connectivity

- Exchange of information is easy and immediate between devices
- As more IT products come to the market, more and more data will be exchanged

# Technology’s Impact on Payments Fraud

## Cloud Systems/ Wi-Fi

93% of Respondents Are Using Cloud



*Source: RightScale 2015 State of the Cloud Report*

*Survey of 930 IT Professionals*

# Technology's Impact on Payments Fraud

## Mobile/ Social

### Mobile

- ➢ Mobile Transactions in US will grow 210% in 2016
  - ○ 2015: mobile payments in U.S. - $8.71 billion
  - ○ 2016: mobile payments in U.S. - $27.05 billion

    *Emarketer 2015*

  - ○ Digital Wallets
    - ■ Smart device purchases online/ in-store
    - ■ Contactless Payments: NFC (Near Field Communication), BLE (Bluetooth Low Energy)
  - ○ Apps
    - ■ In app purchases
    - ■ P2P payments

### Social

- ○ Online purchases: "Buy" buttons monetize user base within social platforms
  - ■ Twitter Buy
- ○ P2P payments
  - ■ Venmo, Snapcash (snapchat, square)
- ○ Attracts fraudsters and provide them huge amounts of data/ users

# Technologies
## Combatting Payments Fraud

### Web Fraud Detection

- Used by organizations that accept/ back payment cards over web (Card-not-present transactions)
- On premises software product or platform; cloud based SaaS
    - Determine whether purchases are made from stolen cards
    - Scans financial transactions made via web/ mobile devices : Modern Risk Analytics

### Who needs Web fraud detection services?

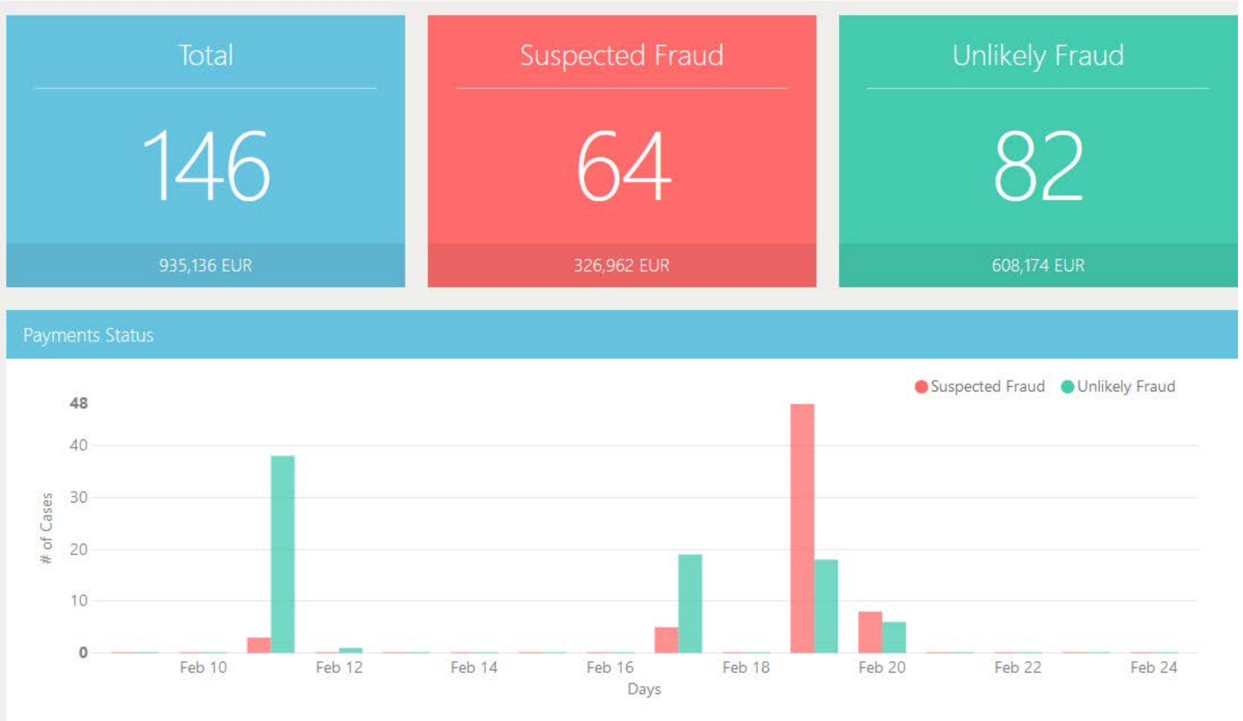
- Organizations of all sizes that deal with any volume of CNP transactions
    - Banking and financial services institutions, e-commerce merchants, human resources and payroll services, social networking sites

# Technologies

## Combatting Payments Fraud

### Modern Risk Analytics

- Analyze transactions in real time
- Determines need for authentication
- Gathers transaction data in flight and creates highly accurate model



- Fraud Score
  - Risk evaluation - scores transactions based on possibility of fraud
  - Tracks unusual patterns of behavior
  - Based on data points
    - User behavior
    - Device ID
    - Geolocation
    - Browser
    - IP address
    - Order links
    - Language setting
    - Frequency of transactions
    - Velocity
    - Size of payments
    - Channel

➢ If transaction falls outside of range, alert is issued, transaction may automatically be suspended/ denied, or cardholder receives call

# Technologies

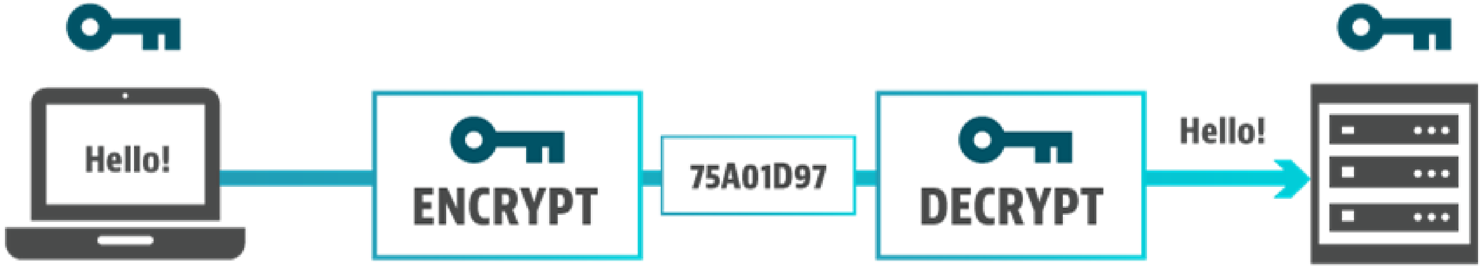
## Combatting Payments Fraud

### Encryption

- Helps keep info secure through mathematical manipulation that renders data unreadable
- Transformation of data via an algorithm
- Data is securely encrypted while being moved from the source to the destination

**Link encryption** -Encrypts and decrypts all traffic at each end of a communication line

**End-to-end encryption** - Message is encrypted by sender at the point of origin and only decrypted by the intended reader



# Technologies

## Combatting Payments Fraud

### Tokenization

- Replacing card's primary account number with random numerical sequence unique to a specific device, merchant, transaction type or channel

- Token mirrors the format of original data in non-descriptive way that can't be mathematically reversed

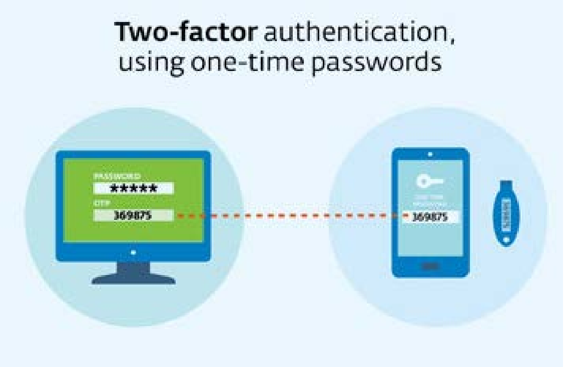
- Data is stored in a safe way and can be accessed and verified for future transactions

# Technologies

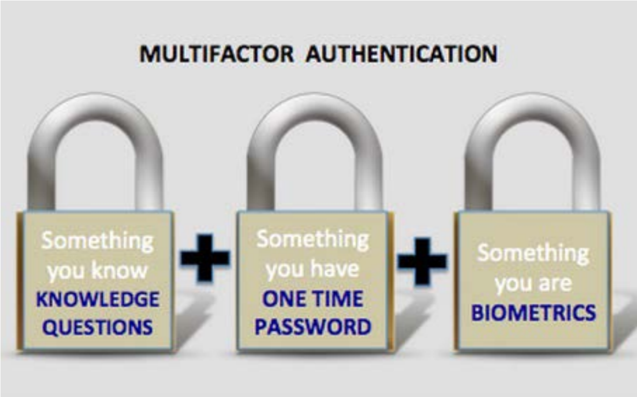
## Combatting Payments Fraud

### Authentication Procedures

- Single Factor Authentication (password to username)
- Two Factor Authentication (verify identity with something you own: mobile)
- Multi Factor Authentication (confirm collection of things to confirm identity)
    - o Biometrics



Con: Increases risk of transaction abandonment


MULTIFACTOR AUTHENTICATION
Something you know KNOWLEDGE QUESTIONS
+
Something you have ONE TIME PASSWORD
+
Something you are BIOMETRICS

European Banking Authority guidelines on Security of Internet Payments

- PSPs must use minimum of two independent authentication elements
- Required to incorporate non-reusable, non-replicable element
- Effort to migrate PSP authentication processes from single-factor to multi-factor

# Technologies

## Combatting Payments Fraud

### 3D Secure

- Each major card brand has 3D Secure solution
  - Verified by Visa, MasterCard SecureCode, American Express SafeKey, etc.
  - Most payment gateways support 3D secure
- Requires cardholder to register their cc with card brand’s 3D solution
- Integrated into business’ website and provides safer online payment method
  - Actual card data not entered on website
  - Cardholder authenticates sale by entering user ID and password (acts like PIN)

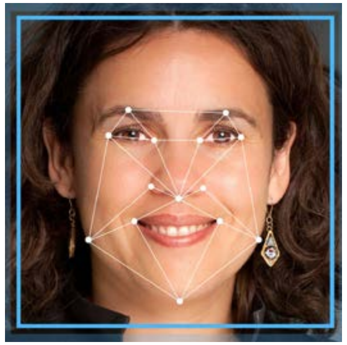
# Technologies

## Combatting Payments Fraud

### Biometric Authentication

- Unique biological characteristics of individuals to verify identity
- Retina scans, fingerscanning, facial recognition, voice identification, etc.

- **Fingerscanning (Fingerprint scanning)**
  - Electronically obtain and store fingerprint
  - Apple Touch ID
    - Unlock device, make purchases, apple pay authentication
  - Concerns exist as relatively new technology
    - Fingerprints last a lifetime → could lead to identity theft and multiple crimes
    - Design flaws- still in infant stages



- **Facial recognition**
  - Faceprints: numeric codes - identify 80 nodal points on face
  - MasterCard (Testing)
    - Popup will ask for authorization after payment: fingerprint or facial recognition
  - Amazon (Filed patent March 10, 2016)
    - System would ask customer to perform action - smile, blink, wink, that can't be replicated with 2 dimensional image

# Recommendations

## Combatting Payments Fraud

*100% protection is impossible → Take necessary steps to avoid it!*

- ➢ Apply security patches
- ➢ Protect networks at every access point
- ➢ Monitor systems & scan for viruses
- ➢ Stronger authentication procedures
- ➢ Establish policy regarding access to confidential information

### If you offer cloud and Internet services:

- Consider devices employees bring to workplace
- Who has access to what info & how data is protected
  - o Periodic sweeps of hosted domains to determine sites listed on known malware distribution lists
  - o Additional security checks during registration process
  - o Limit ability to automate domain registration
  - o Keep systems patched, implement active vulnerability scanning

Make investments now before it is too late!

# Recommendations

## Finding a Solution

- Analyze specific needs
- Evaluate current practices and consider all aspects of security
- Evaluate relationships with other companies
- Evaluate sensitivity of information your business handles
- Consider outlook of your business

## Considerations

- Seamless integrations with other fraud prevention systems
  - Enhance capabilities to optimize fraud prevention
- PCI Compliance
- Layered Security
  - Controls at different points in transaction process
  - Weakness in one control compensated by different control