Payment Card Data and Protected Health Information Security Practices

Andrew Sierra – Merchant Risk
Lester Chan – Merchant Security

August 5, 2015

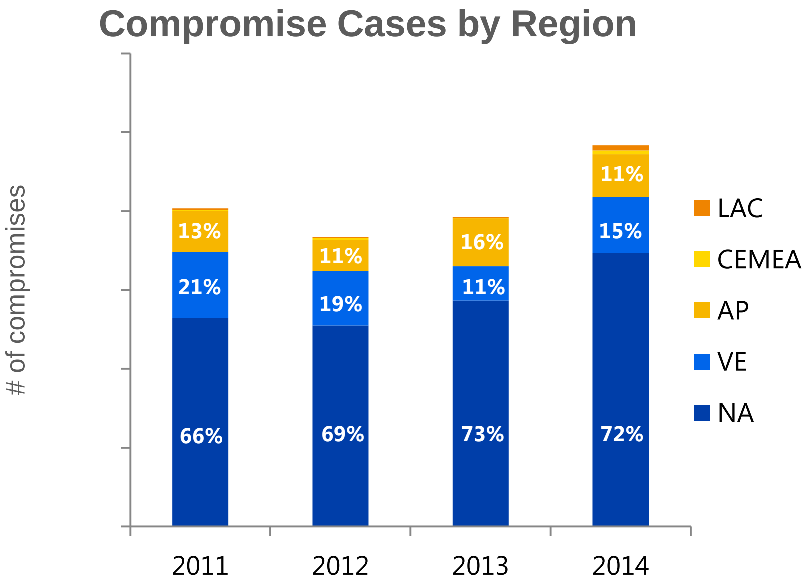
Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- Global Data Compromises
- Cyber Threats and Attacks
- Latest Data Breaches
- Monetizing PII/PHI versus Payment Card Data
- Differences Between Security Standards
- Threats and Risks to Payment Card Data PII/PHI
- Going Above and Beyond Security Standards
- Key Takeaways

Global Data Compromises



- Global data compromise events grew 23% in 2014 over those managed in 2013
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together compromising a quarter of the total
- Breaches in VE and AP are primarily CNP (93% for VE; 94% for AP)

Data Compromises

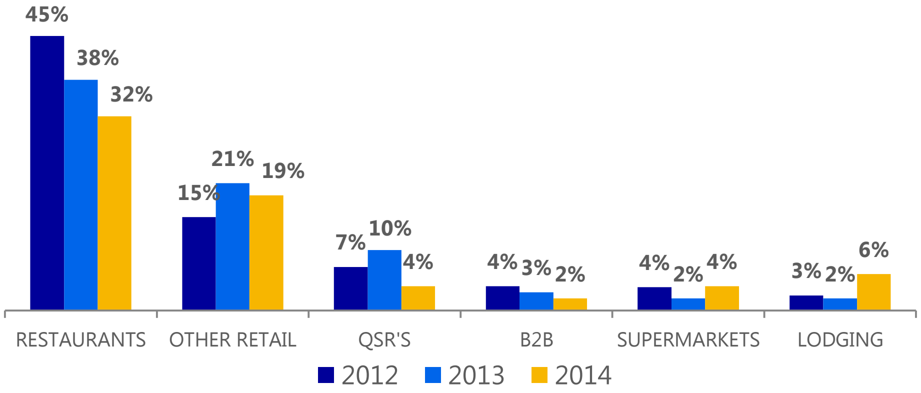
Breach trends by merchant level and Merchant Category Code

Breach Events by Merchant Level

Entity Type		2012	2013	2014
		%	%	%
Merchant	Level 1	<1%	1%	1%
	Level 2	<1%	1%	1%
	Level 3	1%	4%	4%
	Level 4	95%	92%	93%
Agent		<1%	1%	1%
Other		2%	<1%	0%
Total		**100%**	**100%**	**100%**

- While level 4 (small) merchants account for the largest number of known breach events (93% in 2014), the largest impact comes from Level 1 (large) merchant breaches
- Approximately, 77% of at risk accounts in 2014 were tied back to L1 merchants

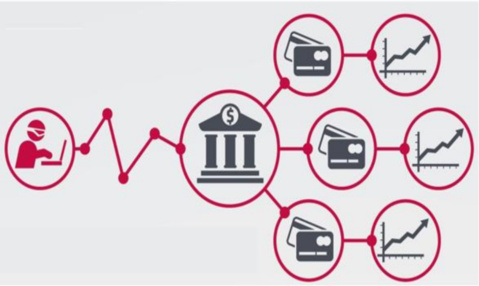
Percent of Breach Events by MCC



- Restaurants and "other retail" make up the biggest portion of total known breaches (32% and 19%, respectively, in 2014)
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs
- High-volume restaurants and retailers continue to be at risk

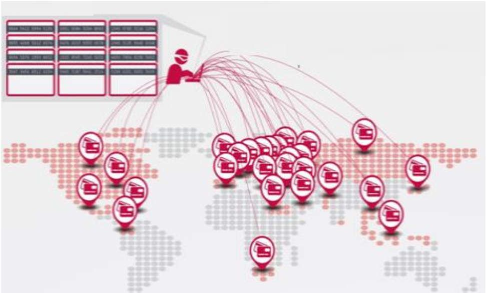
Data Compromises

Common breach patterns



Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, attackers conduct network reconnaissance using diagnostic tools/techniques to identify systems with access to payment data and isolate specific user accounts
- They create custom attack scripts and tools inside the merchant's network to further extend access



Card Data Theft

- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software, in some cases
- Card data is encrypted to avoid detection
- In many recent instances, traces of attacker activity are removed, including self-deleting malware

Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
  - ATMs
  - Gift cards
  - High-value goods
- Cards carry a typical value of between $20-$50 on markets for stolen data

Note: There may be a significant lag between a breach and monetization

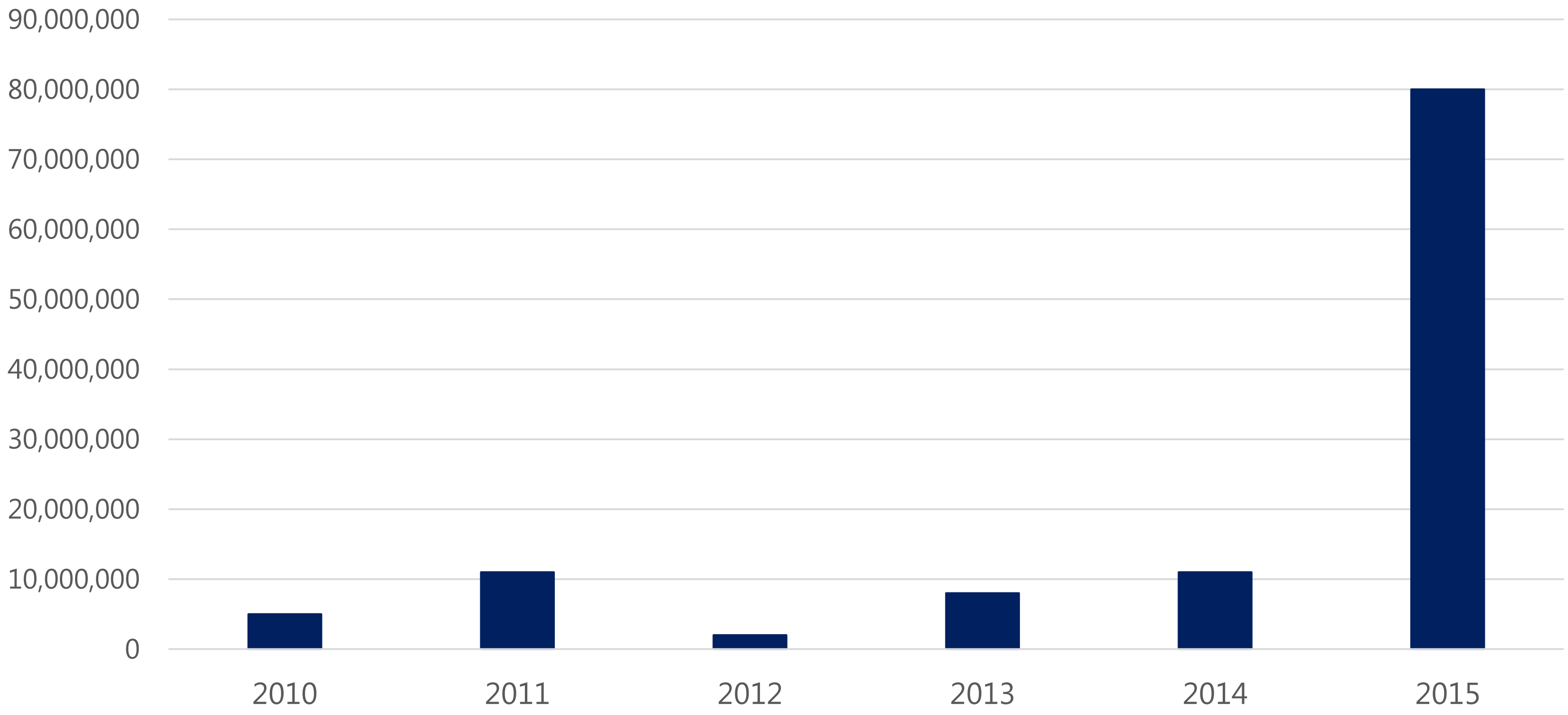
Latest Data Breaches

Lester Chan – Merchant Security

CISSP, CISA, CISM, Certified HIPAA Professional

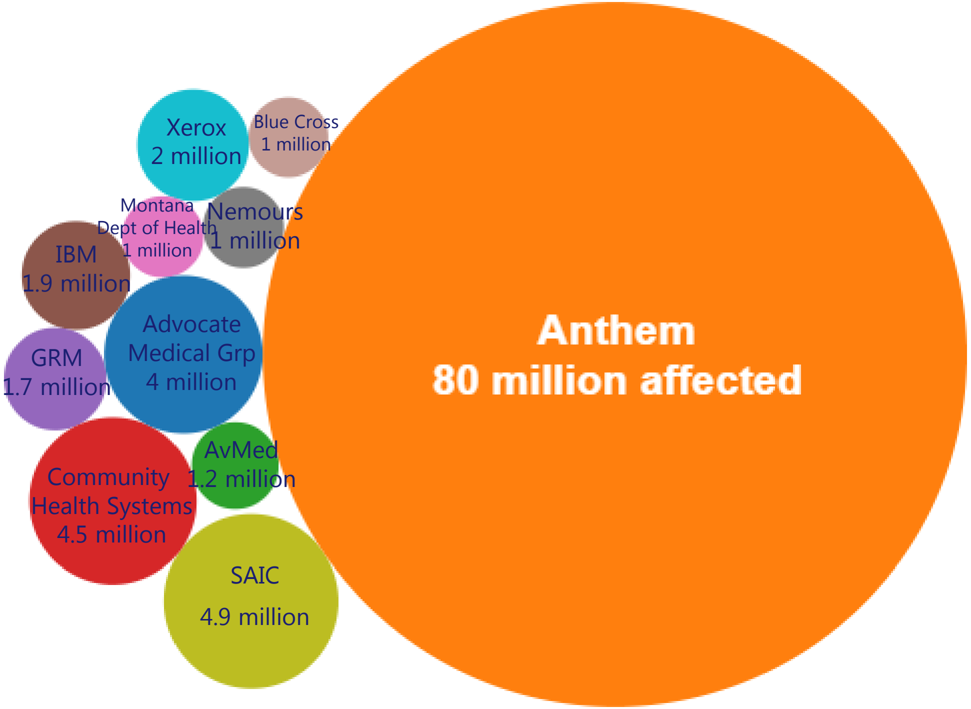
Healthcare Data Breaches Per Year

Number of records



* Source: Forbes, Health Data Breach At Anthem Is A Blockbuster That Could Affect 80 Million, February 5, 2015

Largest Healthcare Data Breaches



Source: HHS Office for Civil Rights

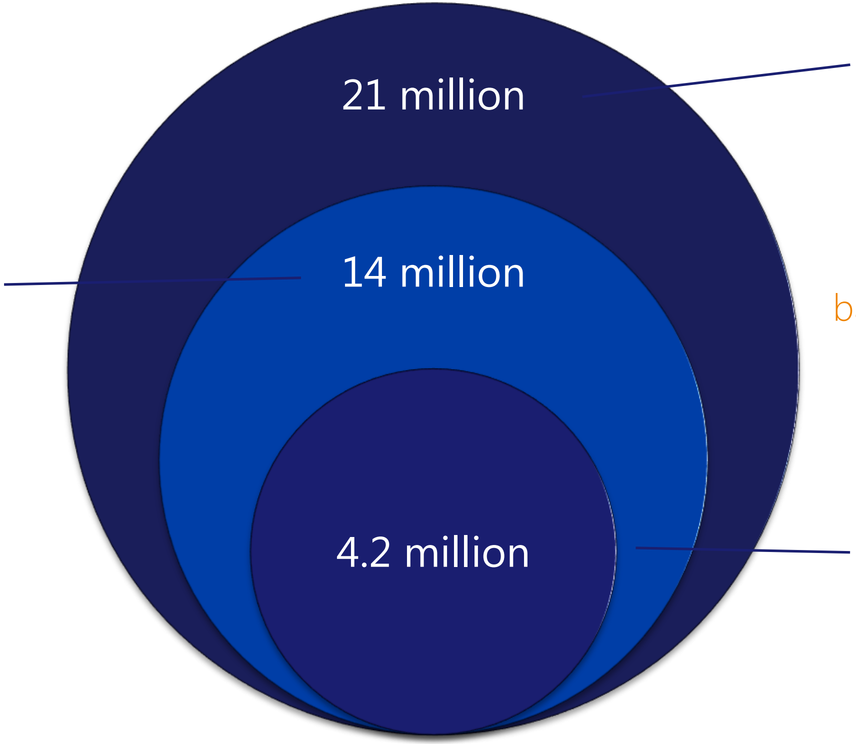
Office of Personnel Management Breach

Not healthcare but PII breach with significant impact

Records include 1.1 million fingerprint records

On June 12, the U.S. government determined an additional 14 million records were stolen by hackers.

The OPM had no dedicated IT security staff until 2013



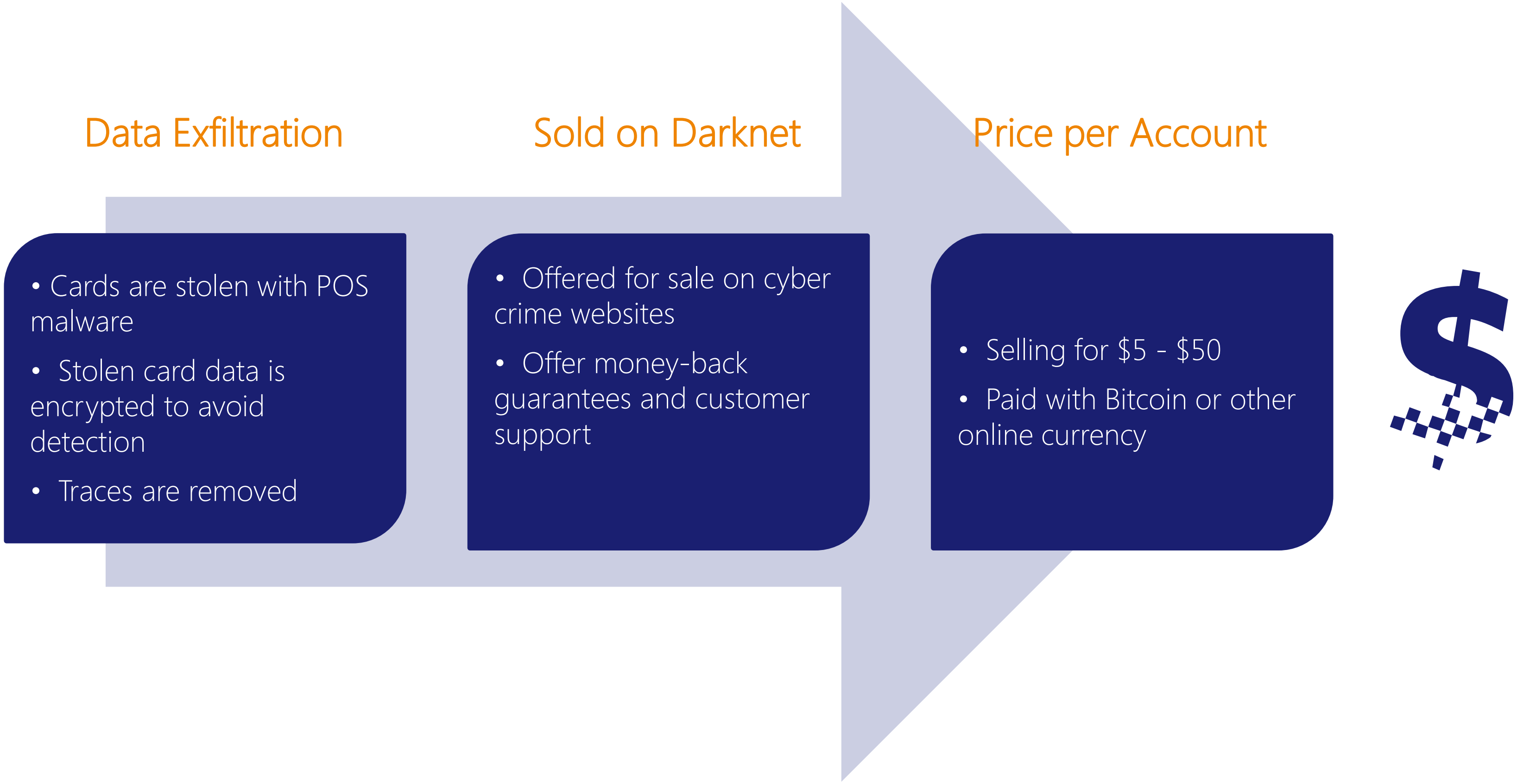
On July 9, OPM discloses that 21 million PII records were compromised by hackers.

Stolen records includes background checks and security clearances for government employees and their families

On June 5, hackers exfiltrated 4.2 million U.S. federal personnel records.

Exfiltration and Monetizing Payment Card Data

Fraudsters can easily monetize stolen payment card data



Data Exfiltration

- Cards are stolen with POS malware
- Stolen card data is encrypted to avoid detection
- Traces are removed

Sold on Darknet

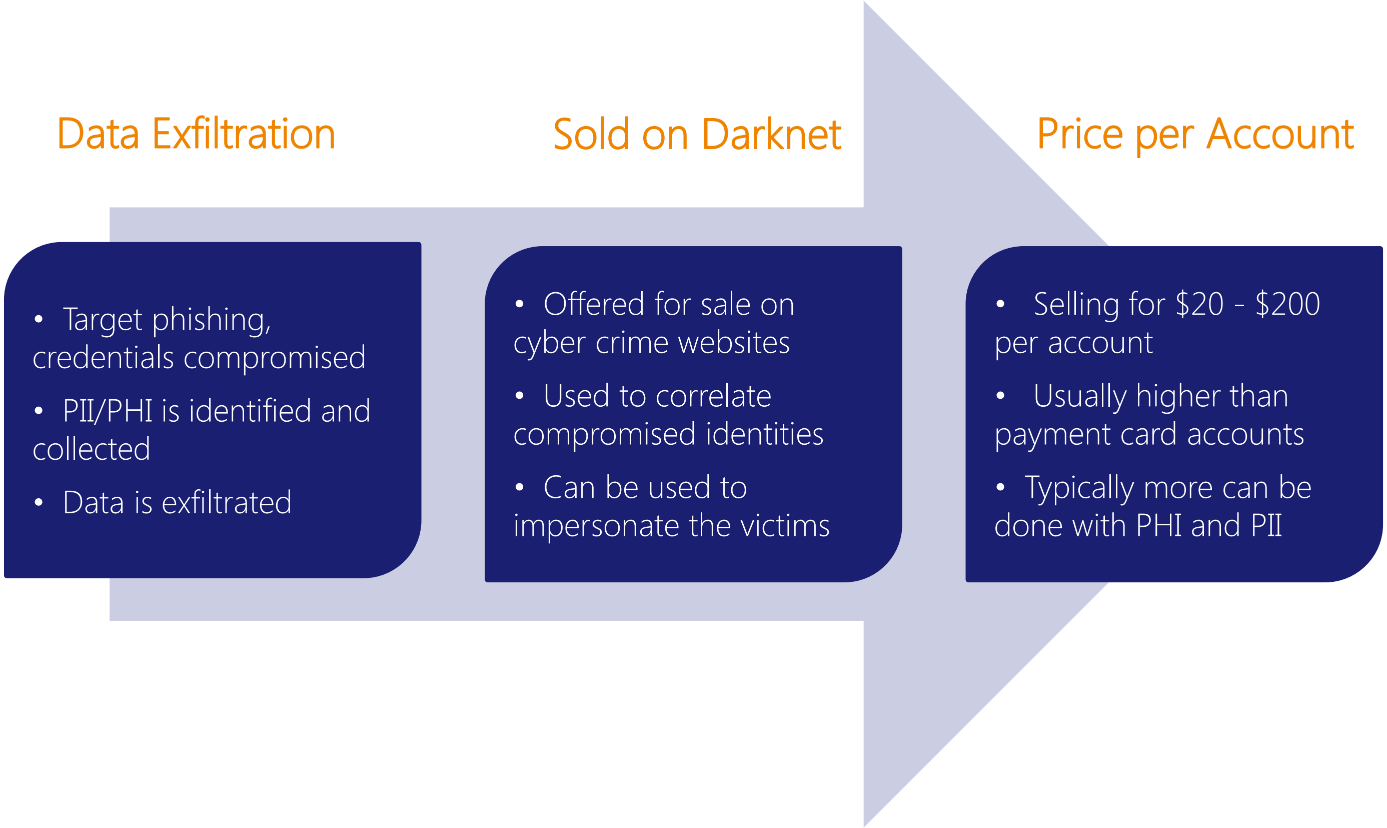
- Offered for sale on cyber crime websites
- Offer money-back guarantees and customer support

Price per Account

- Selling for $5 - $50
- Paid with Bitcoin or other online currency

Exfiltration and Monetizing PII and PHI

Stolen PII/PHI are more useful to fraudsters



Data Exfiltration

- Target phishing, credentials compromised
- PII/PHI is identified and collected
- Data is exfiltrated

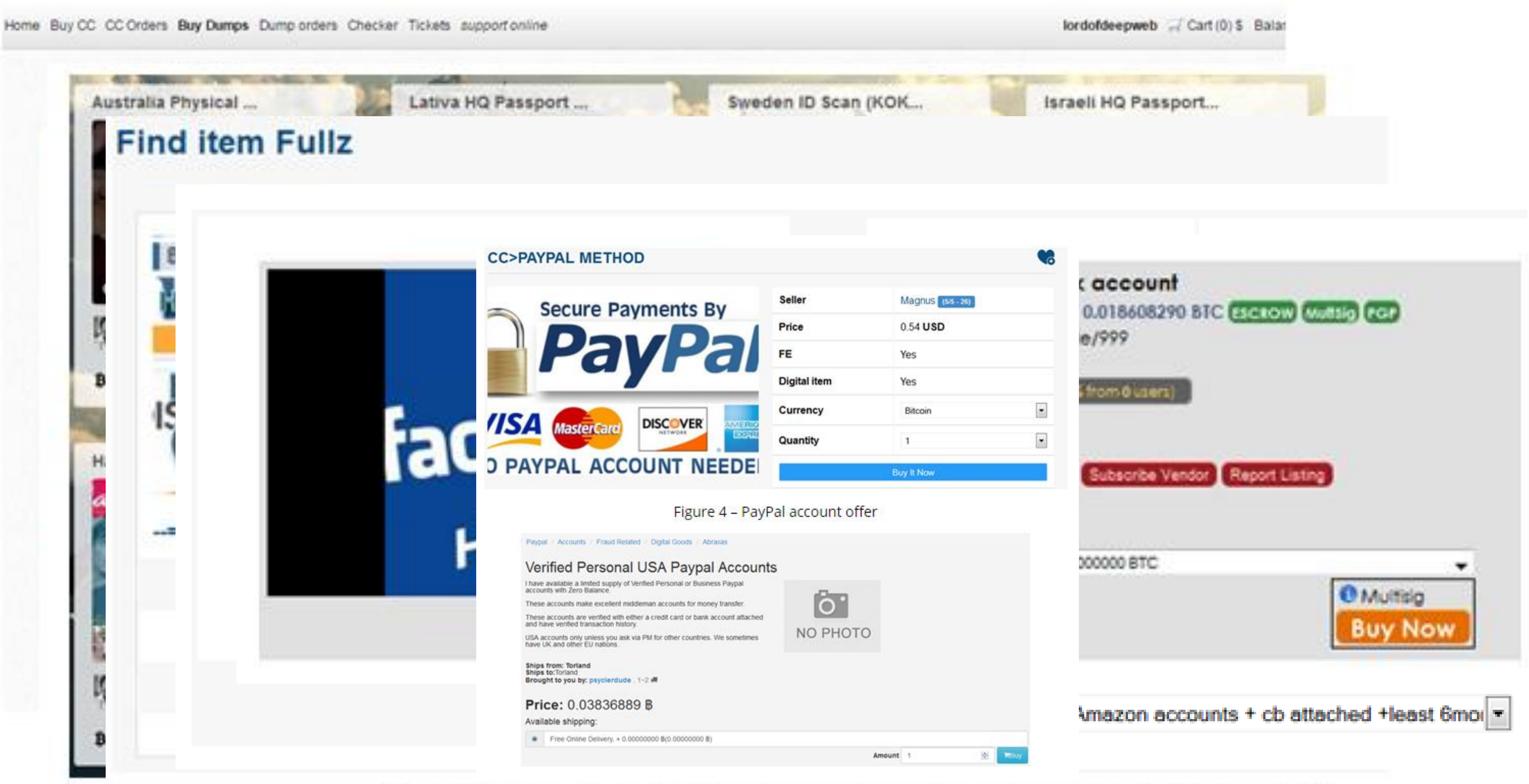
Sold on Darknet

- Offered for sale on cyber crime websites
- Used to correlate compromised identities
- Can be used to impersonate the victims

Price per Account

- Selling for $20 - $200 per account
- Usually higher than payment card accounts
- Typically more can be done with PHI and PII

Dumps, "Fullz", and Payment Card Data on the Darknet



Home Buy CC CC Orders Buy Dumps Dump orders Checker Tickets support online
lordofdeepweb Cart (0) $ Balar
Australia Physical ...
Lativa HQ Passport ...
Sweden ID Scan (KOK...
Israeli HQ Passport...
Find item Fullz
CC>PAYPAL METHOD
Secure Payments By PayPal
VISA MasterCard DISCOVER
O PAYPAL ACCOUNT NEEDE
Buy It Now
account
0.018608290 BTC ESCROW Multisig PGP
e/999
from 0 users)
Subscribe Vendor Report Listing
000000 BTC
Multisig
Buy Now
Amazon accounts + cb attached +least 6mo

Seller	Magnus (5/5 - 26)
Price	0.54 USD
FE	Yes
Digital item	Yes
Currency	Bitcoin
Quantity	1

Figure 4 – PayPal account offer

Paypal / Accounts / Fraud Related / Digital Goods / Abraxas

Verified Personal USA Paypal Accounts

I have available a limited supply of Verified Personal or Business Paypal accounts with Zero Balance.

These accounts make excellent middleman accounts for money transfer.

These accounts are verified with either a credit card or bank account attached and have verified transaction history.

USA accounts only unless you ask via PM for other countries. We sometimes have UK and other EU nations.

Ships from: Torland
Ships to: Torland
Brought to you by: psyclerdude , 1~2

NO PHOTO

Price: 0.03836889 ฿

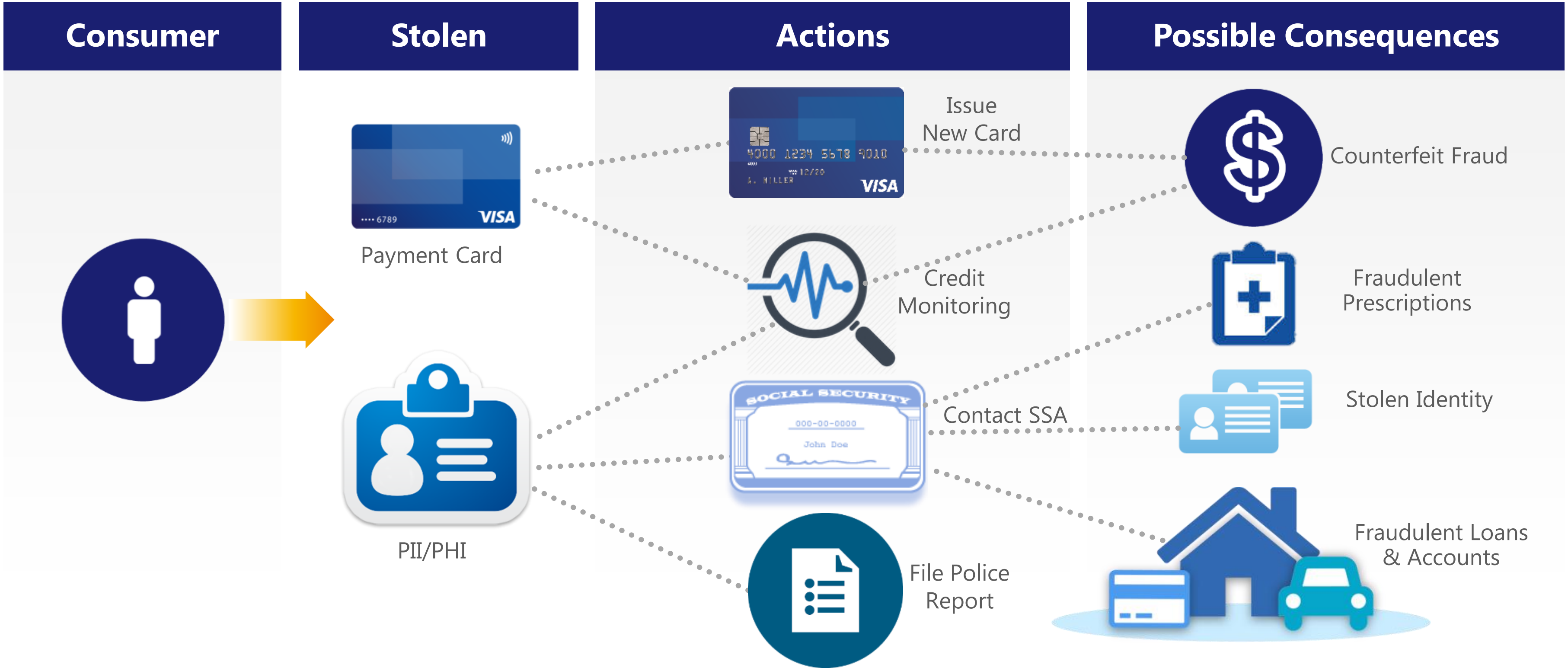
Available shipping:

● Free Online Delivery, + 0.00000000 ฿(0.00000000 ฿)

Amount 1 Buy

Breach Impact to Victims

Significant impact to victims of payment card fraud and PII/PHI theft



Consumer

Stolen

Actions

Possible Consequences

Payment Card

PII/PHI

Issue New Card

Credit Monitoring

Contact SSA

File Police Report

Counterfeit Fraud

Fraudulent Prescriptions

Stolen Identity

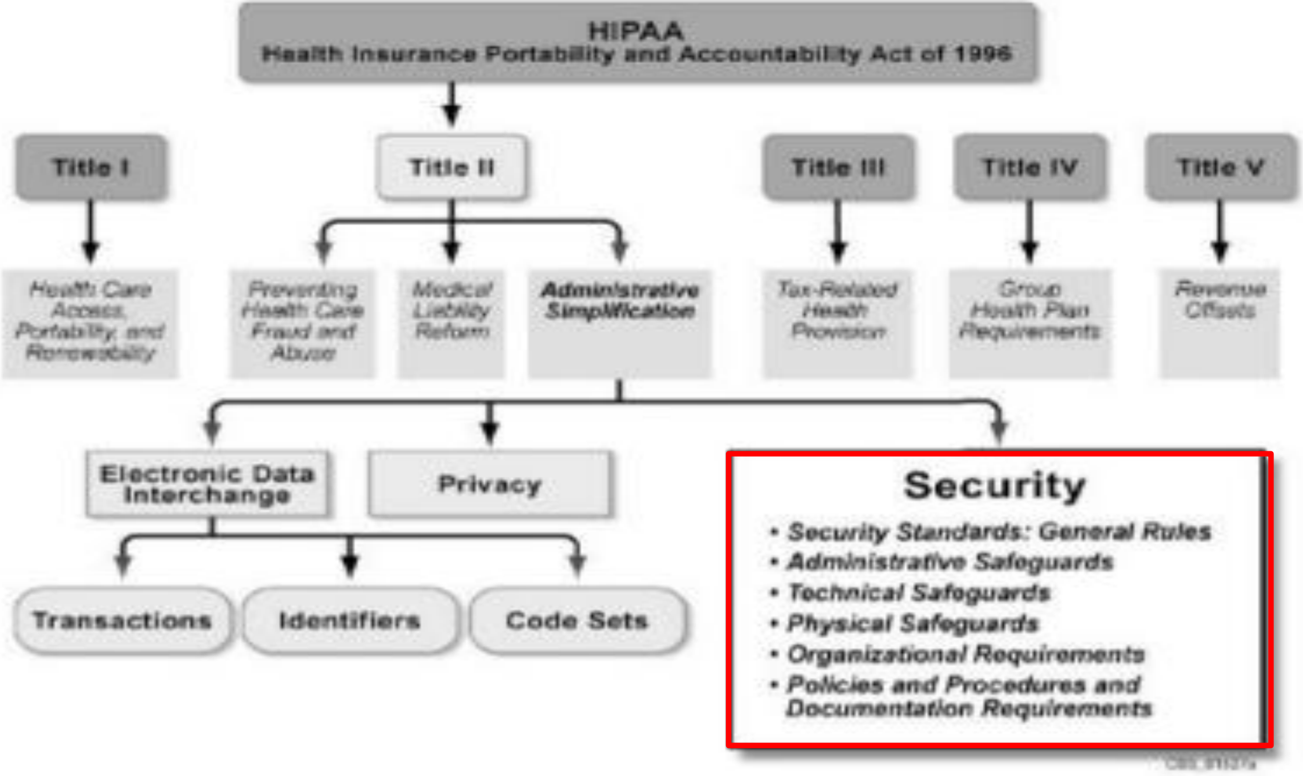
Fraudulent Loans & Accounts

Payment Card Industry (PCI) Data Security Standard (DSS)

Health Insurance Portability and Accountability Act (HIPAA) Security

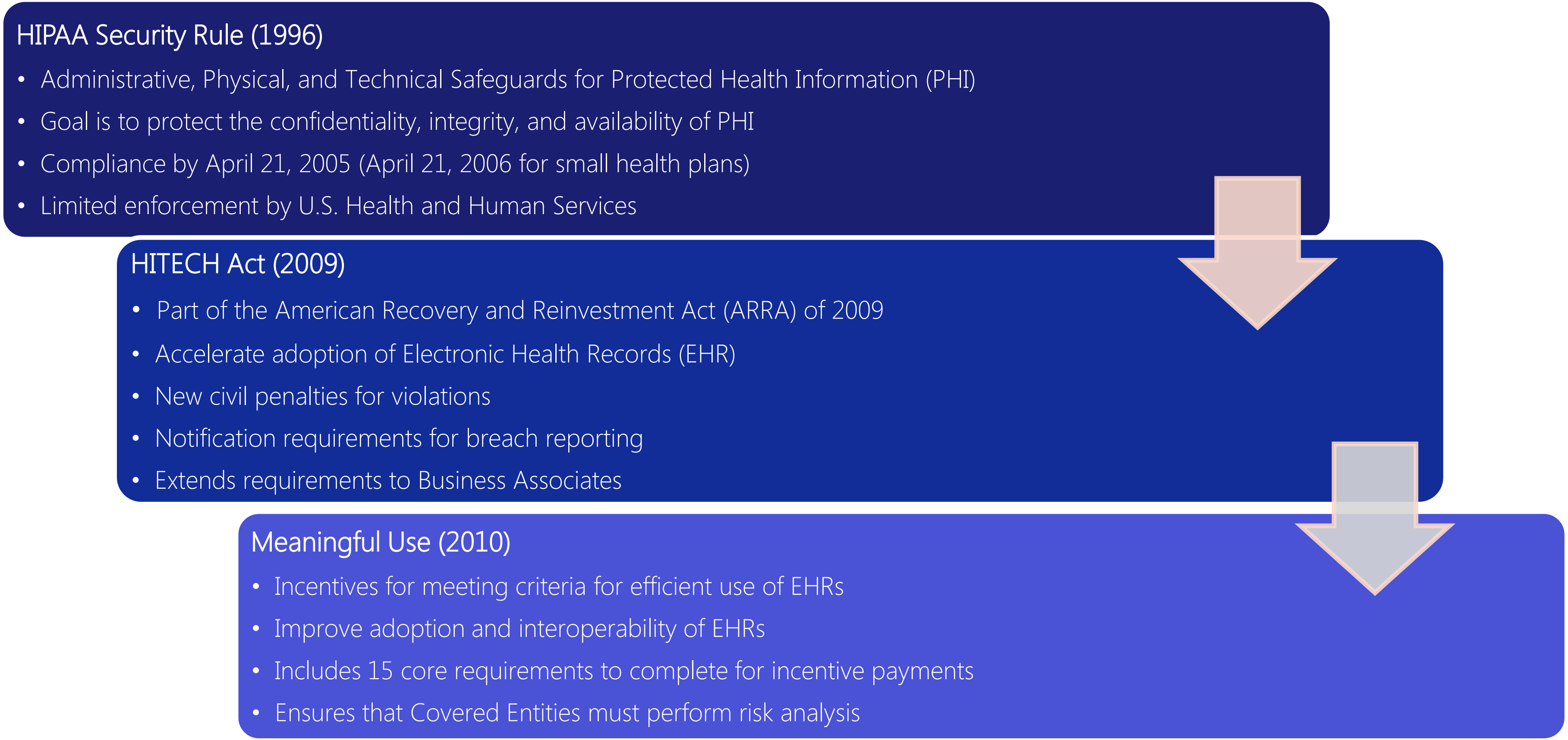
Health Insurance Portability and Accountability Act

HIPAA Security is one section of the HIPAA Rule


HIPAA
Health Insurance Portability and Accountability Act of 1996
Title I
Title II
Title III
Title IV
Title V
Health Care Access, Portability, and Renewability
Preventing Health Care Fraud and Abuse
Medical Liability Reform
Administrative Simplification
Tax-Related Health Provision
Group Health Plan Requirements
Revenue Offsets
Electronic Data Interchange
Privacy
Transactions
Identifiers
Code Sets
Security

- Security Standards: General Rules
- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

Regulatory Requirements for Healthcare Data



HIPAA Security Rule (1996)

- Administrative, Physical, and Technical Safeguards for Protected Health Information (PHI)
- Goal is to protect the confidentiality, integrity, and availability of PHI
- Compliance by April 21, 2005 (April 21, 2006 for small health plans)
- Limited enforcement by U.S. Health and Human Services

HITECH Act (2009)

- Part of the American Recovery and Reinvestment Act (ARRA) of 2009
- Accelerate adoption of Electronic Health Records (EHR)
- New civil penalties for violations
- Notification requirements for breach reporting
- Extends requirements to Business Associates

Meaningful Use (2010)

- Incentives for meeting criteria for efficient use of EHRs
- Improve adoption and interoperability of EHRs
- Includes 15 core requirements to complete for incentive payments
- Ensures that Covered Entities must perform risk analysis

PCI Security Standards Council (PCI SSC)

VISA

1 Industry-wide standards group founded in 2006

Visa, American Express, Discover, JCB and MasterCard

3 PCI DSS applies to any entity that stores, processes, or transmits cardholder data

2 Responsible for development and management of PCI Security Standards

PCI DSS, PA-DSS, and PTS

4 Trains and certifies data security companies

ASVs, QSAs, PA-QSAs, and PFIs

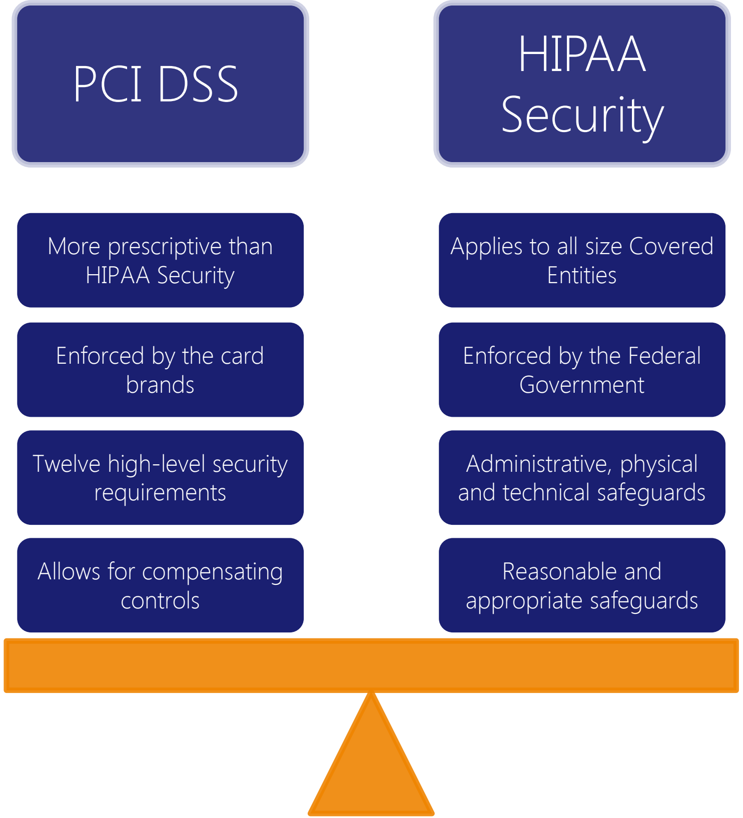
PCi Security Standards Council™

www.pcisecuritystandards.org

Differences between PCI DSS and HIPAA Security

Key differences in security standards

- Store, process, or transmit payment card data
- Requires self assessment questionnaire for small merchants
- QSA or ISA for large merchants
- Requires vulnerability scanning and pentesting



PCI DSS

More prescriptive than HIPAA Security

Enforced by the card brands

Twelve high-level security requirements

Allows for compensating controls

HIPAA Security

Applies to all size Covered Entities

Enforced by the Federal Government

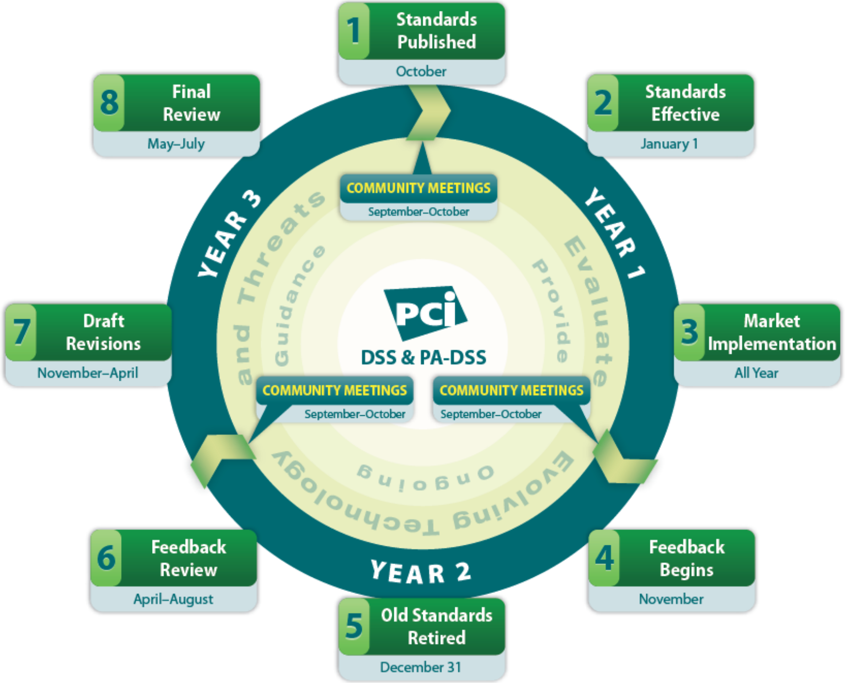
Administrative, physical and technical safeguards

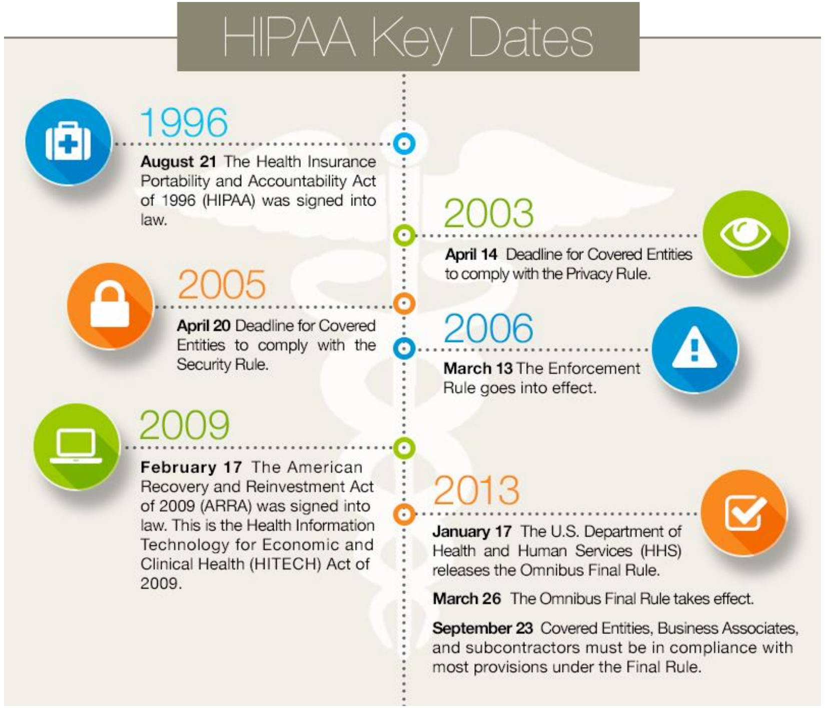
Reasonable and appropriate safeguards

- Applies to Covered Entities
- Penalties can include civil and criminal
- Required versus addressable
- Either stored or transmitted
- Applies to Business Associates
- Document policies and procedures

Changes to PCI DSS Versus HIPAA Security

VISA





HIPAA Key Dates

1996

August 21 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law.

2003

April 14 Deadline for Covered Entities to comply with the Privacy Rule.

2005

April 20 Deadline for Covered Entities to comply with the Security Rule.

2006

March 13 The Enforcement Rule goes into effect.

2009

February 17 The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law. This is the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

2013

January 17 The U.S. Department of Health and Human Services (HHS) releases the Omnibus Final Rule.

March 26 The Omnibus Final Rule takes effect.

September 23 Covered Entities, Business Associates, and subcontractors must be in compliance with most provisions under the Final Rule.

Staying ahead latest threats and risks

Going Above and Beyond PCI DSS and HIPAA Security

Threats and Risks to Payment Card Data and PII/PHI

Targeted attacks and growing threats

Targeting companies with low security

Exploit weaknesses with root kits, POS malware

Database stores of payment card data and/or PII/PHI

Email attachments with various exploits

Keyloggers used to harvest login credentials

Buffer overflows attacks to create backdoors on systems

Improve e-commerce security and ensure application security controls are used

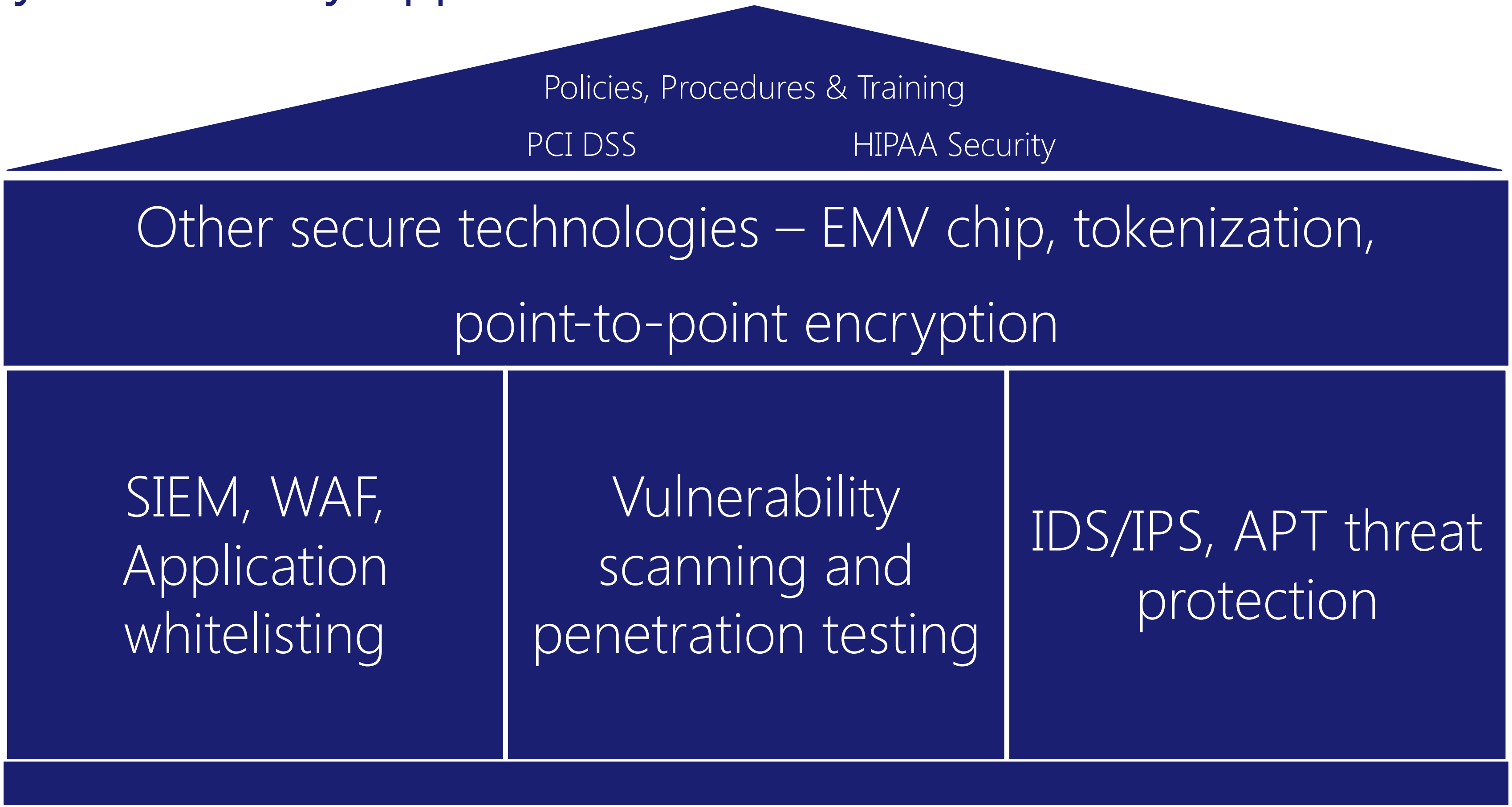
Merchants accepting mag stripe transactions will be targeted

Security Standards Compliance

Higher education, hospitals, etc. have multiple regulatory requirements

- Hospitals have HIPAA, JCAHO, PCI DSS, Sarbanes-Oxley, FDA, etc.
- Some are challenging environments to assess, multiple locations, stores, parking, kiosks, etc.
- Validate compliance independently but leverage key activities
- Executive sponsorship is a must
- Document all findings especially risk assessment, gap analysis, and key controls

Layered Security Approach



Policies, Procedures & Training

PCI DSS

HIPAA Security

Other secure technologies – EMV chip, tokenization, point-to-point encryption

SIEM, WAF, Application whitelisting

Vulnerability scanning and penetration testing

IDS/IPS, APT threat protection

Maturing Information Security

Validate to Version 3.1

After April 2015, all merchants must validate to PCI DSS version 3.1.

Version 3.1 continues to evolve the PCI DSS standard controls to address current threats and vulnerabilities.

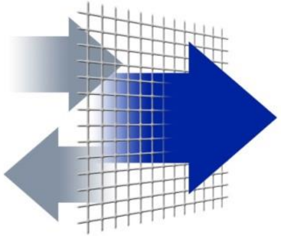
Note the penetration testing requirement (11.3) effective after June 30, 2015.

Implement P2PE, EMV Chip, and Tokenization

EMV Chip - Creates a unique cryptogram for each transaction

Tokenization - Token replaces account number with unique digital token

P2PE -Encrypt from the point of sale to the point where the third-party payment processor or acquirer decrypts the data for processing



Proactive Security Controls

- Use two-factor authentication especially for remote access
- File integrity monitoring to protect against malware
- Application whitelisting to allow only those allowed applications
- Improve segmentation between CDE and core network
- Web application firewalls (WAF)
- Properly segment CDE

Additional Security Controls for Large Merchants

SIEM

- Security intelligence and correlation
- Alerts and notification
- Tuning

Vulnerability Management

- Frequency of scans
- Zero day vulnerabilities
- Remediation and tracking

Antivirus

- Keep signatures updated
- Ensure settings cannot be altered

Patch Management

- Keep all software, hardware, appliances up to date
- End of life systems
- Vulnerability window

Examples of Small Merchant Security Safeguards*

1.

2.

3.

4.

5.

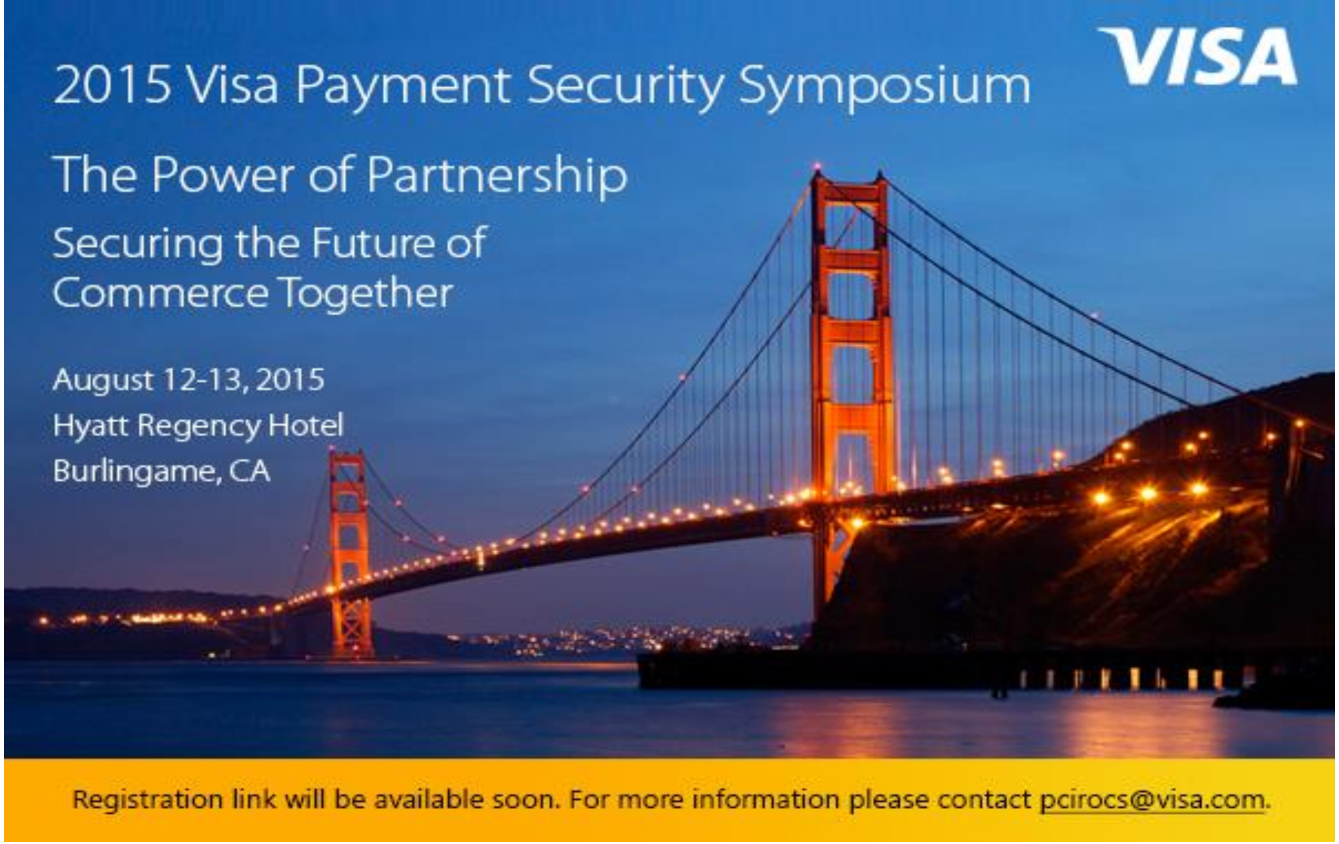
	Change Default Passwords	Install Antivirus	Enable Remote Access Only When Needed	Segment Network	Conduct Employee Training & Awareness
Ease of Implementation	Easy	Medium	Easy	Medium	Easy
Cost	None	Medium	None	Medium	Low
Effectiveness	Medium	Medium	High	High	High

*Based on PCI Forensic Investigation Reports of Small Merchants

Key Takeaways

Lessons Learned

1. **PII/PHI versus payment card data** – PII/PHI is typically worth more on the darknet than payment card data
2. **Hackers targeting path of least resistance** – Hackers know companies that have weak or low security controls
3. **After liability shift, fraud will migrate to other channels** – Shift to card not present channels such as e-commerce
4. **Devalue the data** – Make payment card data, PII/PHI unusable to fraudsters when compromised
5. **Implement secure technology** – Consider point-to-point encryption, tokenization, and EMV chip to protect data
6. **Go above PCI DSS and HIPAA Security** – Both security standards are a floor, not ceiling, implement complimentary controls for a layered security approach



2015 Visa Payment Security Symposium

The Power of Partnership

Securing the Future of
Commerce Together

August 12-13, 2015
Hyatt Regency Hotel
Burlingame, CA

Registration link will be available soon. For more information please contact pcirocs@visa.com.

Visa is hosting a must-attend event that will focus on trends and developments related to cyber security, mobile payments, e-commerce and Visa’s global authentication strategy. In order to secure the future of commerce all stakeholders including merchants, acquirers, agents and Visa need to collaborate on key initiatives in addressing today’s most relevant issues. This event will be held in the San Francisco Bay Area at the Hyatt Regency Hotel just south of San Francisco.

Upcoming Events and Resources

Upcoming Webinars – Under Merchant Resources/Training on www.visa.com

- Implementing Effective Penetration Testing, August 25, 2015
- The Importance of Containment and Remediation of Compromised Payment Processing Environments, September 2, 2015

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration – www.VisaChip.com/businesstoolkit

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards, QIR Listing
- Fact Sheets –Mobile Payments Acceptance, Tokenization, and many more…

Thank you for attending!

Questions? Comments?

VISA