Friend or Foe? How to detect medical identity thieves on your online portal

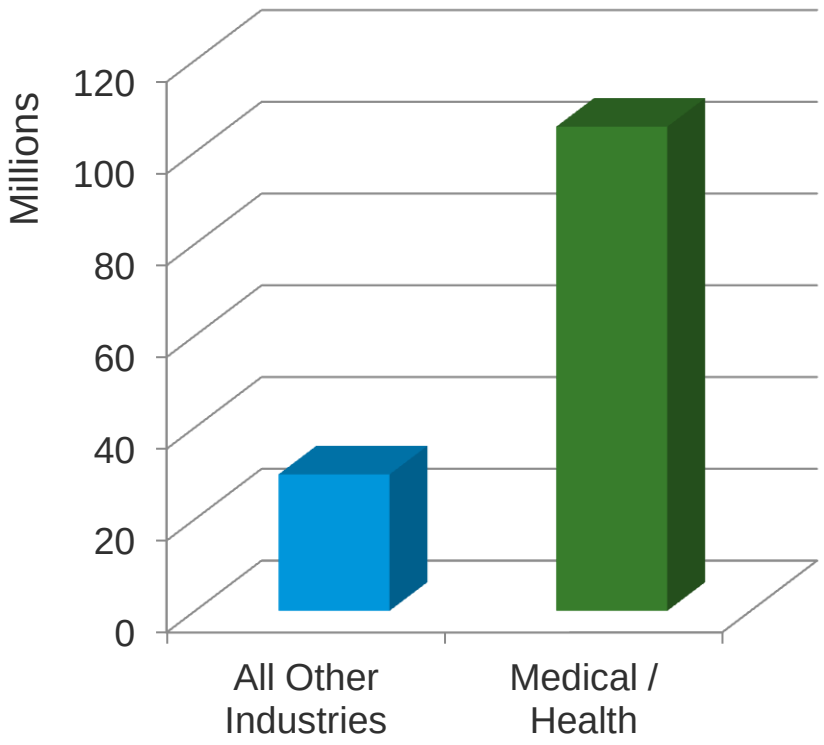
Elazar Katz, VP Strategic Initiatives,
Experian Health

Healthcare has become the #1 target

2015 Trends

- **105.5 MM** records have been compromised thus far in 2015; versus 8.3 MM in 2014
- Medical identity theft is the fastest growing type of identity theft, growing at 22% annually.
- **1 in 3 Americans** has been affected by a large health data breach
- Criminal attacks are the number one cause of healthcare breaches

Number of compromised records 2015*



Experian Health

PASSPORT A part of Experian

Source: Identity Theft Resource Center, July 2015 report
**2015 numbers are through 7/28/15*

Medical data has become harder to protect

INCREASING VOLUME

Increasing volume of PHI on data storage platforms

FLUID & MOBILE

Fluidity and persistence of data on computers, mobile devices and internet

DATA IS LUCRATIVE

Medical identities are more lucrative than financial identities

THEFT HARDER TO DETECT

It can take up to one or two years before medical identity theft is detected.

Experian Health

PASSPORT A part of Experian

Network breaches open the door for portal breaches

- Stolen information is used to impersonate individuals and gain access to portals
- While the memory of a breach fades, **the risk to portals and consumers remains**
- Lack of detection tools makes healthcare portals a ripe target

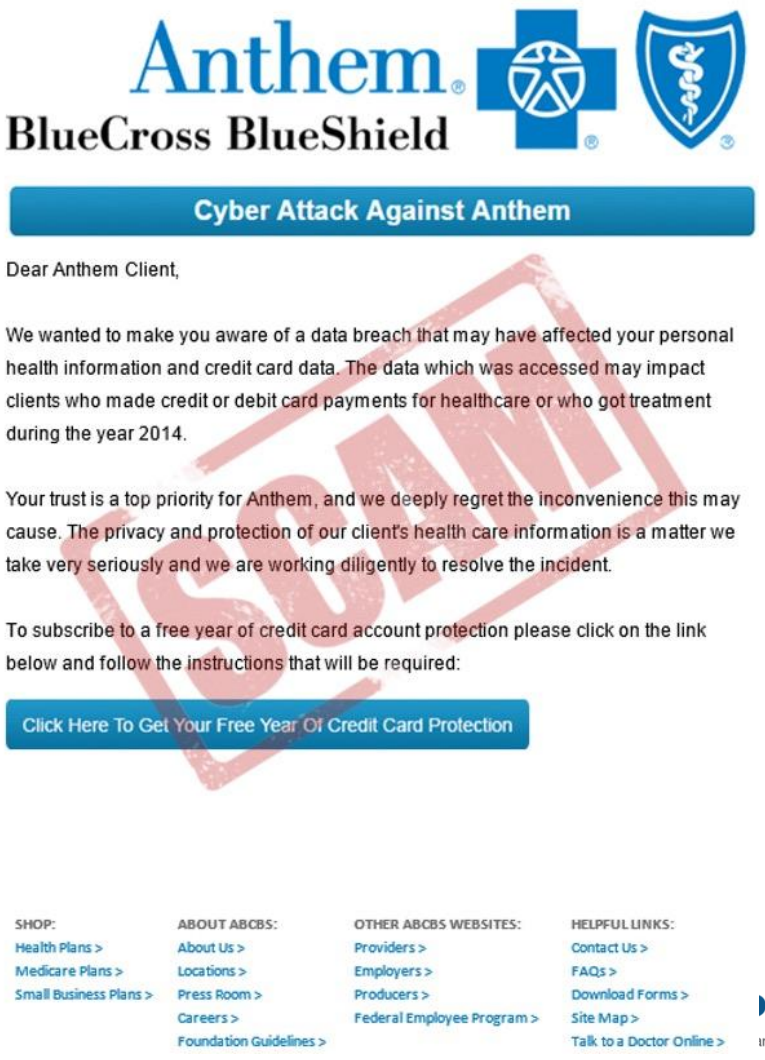
One-stop shop	• Portal designed to break silos • Multiple systems and servers accessed
All patients are at risk	• Not only those that enrolled in portal • Fraudsters can enroll additional patients
All portals impacted	• Identities stolen from one institution can be used in the portal of another

Experian Health

PASSPORT A part of Experian

Attack Method: Phishing

- Can leverages information stolen in breach
- Can be done via text, email, phone calls, etc.
- Used to obtain additional information such as:
  - Credit card
  - Social security number
  - Phone
  - Personal Information



- In 2013, **450,000** phishing attacks
- Estimated losses of **$5.9 billion**

Experian Health

Source: RSA 2013 A Year in Review Fraud Report

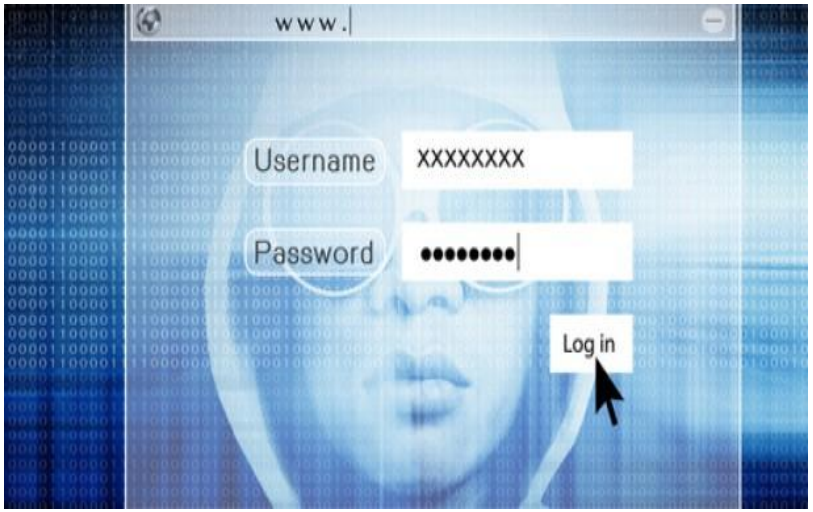
Attack method: key-logging Trojans

Consistent URL text strings make portals more vulnerable

Banking Trojans can be easily configured to target patient portals

6% of broadband residential customers are infected with high-level threats such as bots, root-kits, and banking Trojans*

20% Increase in infection of mobile devices in 2013*



4 “Big four” banking Trojans (Carberp, Citadel, SpyEye, and Zeuss) can be easily converted to target patient portals

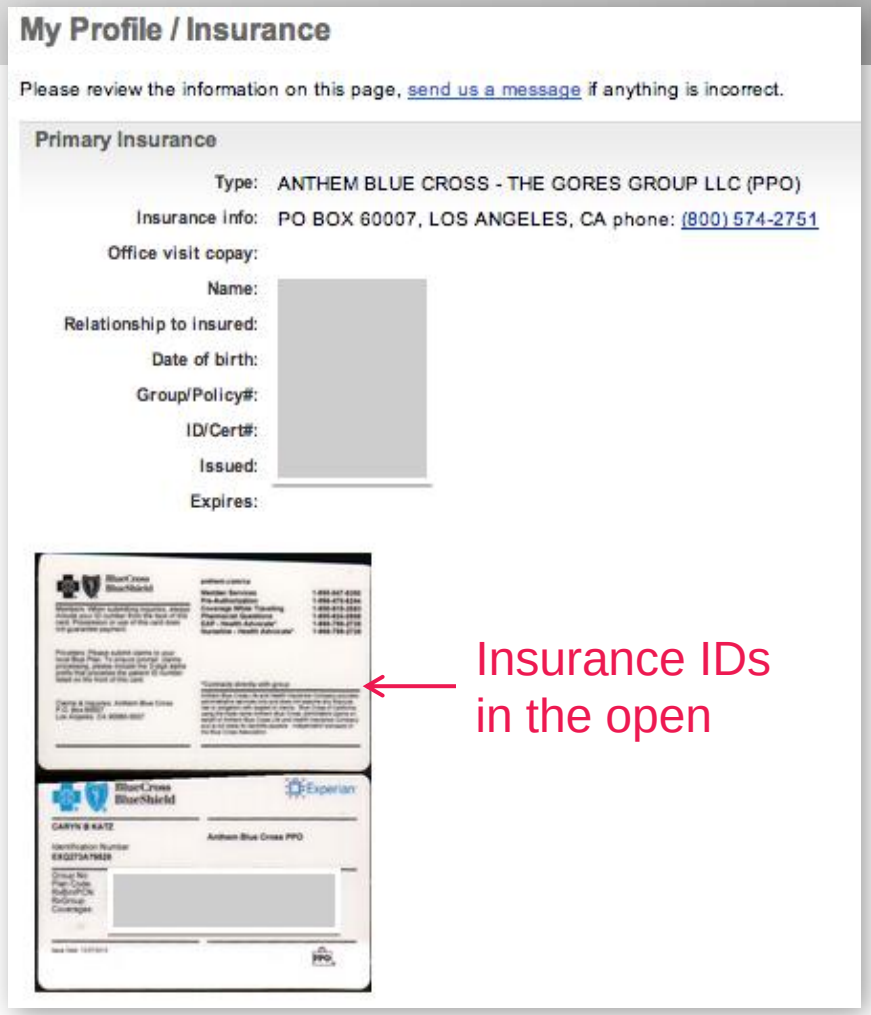
Experian Health

PASSPORT A part of Experian

Source: Alcatel-Lucent Kindsight Security Labs Malware Report Q4 2013

Aggravating factor: Many portal designs ignore basic security

- Personal and medical identities are presented in the clear
- No covert login- monitoring, widely used in online banking
- Compromise-detection processes are immature and lead to delayed detection
- It is often over a year before medical ID theft is discovered



Experian Health

PASSPORT A part of Experian

Aggravating factor: mandated “problem list”

Simplifies classification of victims by type of fraud they could support

Problem Lists enable easy classification of victims

- Mandated “problem list” describes patient’s ailments
- Use of standard terminology (ICD-9 CM or SNOMED CT standards) enables malware to search by keywords and sort victims by the type of fraud they could support

		Start Date	Code	Diagnosis	Comments	End Date
		Mar-18-2008	784.0	HEADACHE	associated with nausea	May-14-2008
		Aug-04-2006	401	ESSENTIAL HYPERTENSION	cured	Sep-06-2006
☐		Jul-27-2006	278.00	OBESITY UNSPECIFIED	WELL BABY	
☐		Jul-16-2005	272.2	MIXED HYPERLIPIDEMIA	Got myalgias once with Lopid	
☐		Jul-24-2002	250	DIABETES MELLITUS	Not required insulin until 2005	
☐		Aug-22-2001	401	ESSENTIAL HYPERTENSION	Not well controlled during the first 3 years	

Experian Health

PASSPORT A part of Experian

Lack of monitoring tools worsens the impact of medical identity theft

- **Reputational costs**
  - Publicized sensitive medical info
- **Health costs**
  - Emotional distress
  - Discontinued health care / benefits
  - Denial of prescription medication
- **Financial costs:**
  - On average victims spent over **$13,500 and 210 hours** to resolve their compromise.
    - 20% of their household income

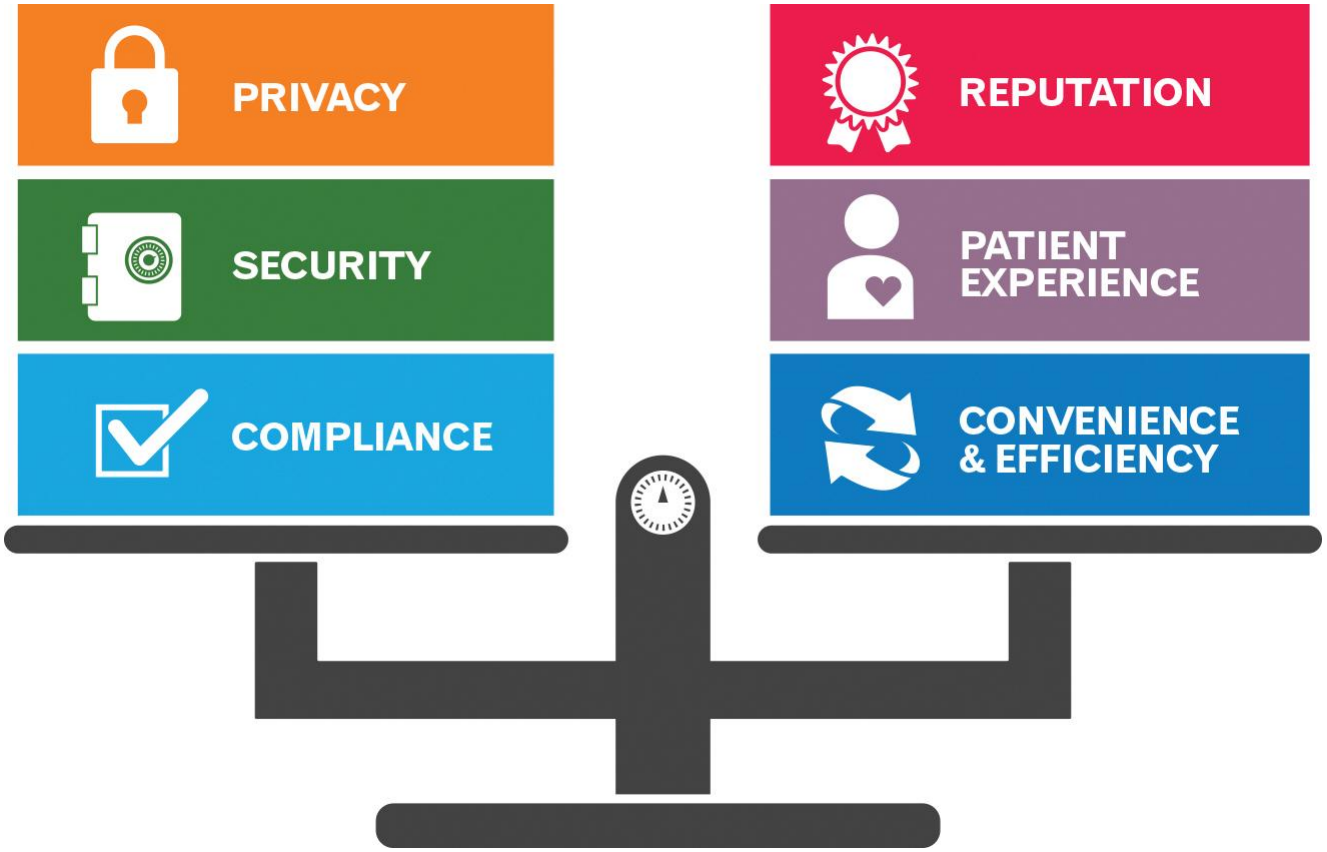
- **Reputational costs**
  - Degraded brand image
  - Consumer distrust
- **Financial costs**
  - Breach retribution costs
  - HIPAA fines up to $1.5M per violation
  - Legal costs
  - Loss of current and future patients
  - Malpractice lawsuits from misdiagnosis and treatment

Experian Health

PASSPORT A part of Experian

Source: 2013 Survey On Medical Identity Theft, Ponemon Institute

The challenge is balancing security and patient experience



We balance it all.

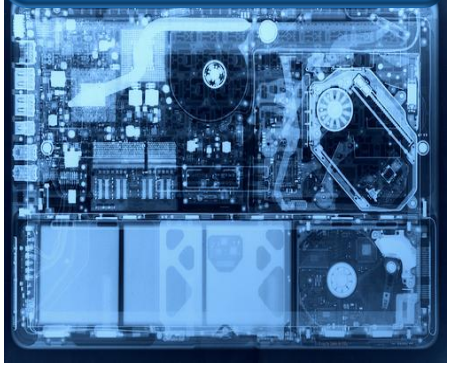
Experian Health

PASSPORT A part of Experian

The key is leveraging a multi-layered approach

Identity

Device Trust & Compatibility



Hostile Device Behavior

Criminal History

Leverage identity and device intelligence and separate friend from foe

Experian Health

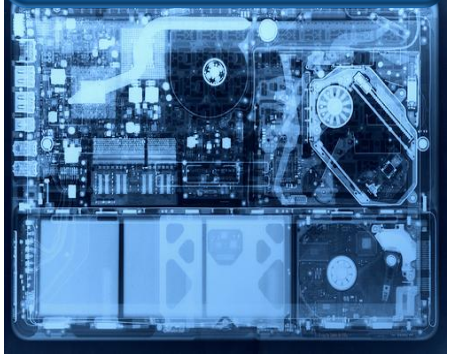
PASSPORT
A part of Experian

The key is leveraging a multi-layered approach

Identity

- Knowledge-based authentication
- Excessive permutations of identity information
- Identity associated with fraud

Device Trust & Compatibility



Hostile Device Behavior

Criminal History

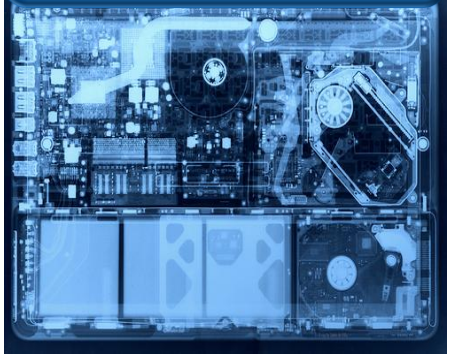
PASSPORT
A part of Experian

The key is leveraging a multi-layered approach

Identity

- Knowledge-based authentication
- Excessive permutations of identity information
- Identity associated with fraud

Device Trust & Compatibility



- History of device with user
- Configuration incompatible with user preferences
- Internal incompatibilities

Hostile Device Behavior

Criminal History

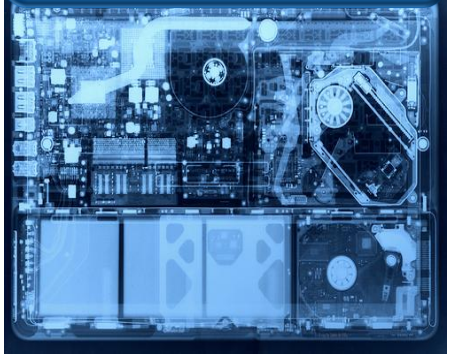
PASSPORT
A part of Experian

The key is leveraging a multi-layered approach

Identity

- Knowledge-based authentication
- Excessive permutations of identity information
- Identity associated with fraud

Device Trust & Compatibility



- History of device with user
- Configuration incompatible with user preferences
- Internal incompatibilities

Hostile Device Behavior

- Impersonate multiple identities
- Represent multiple identities while not being trusted by them
- Repeat infrequent activities (e.g. changing phone # or email)

Criminal History

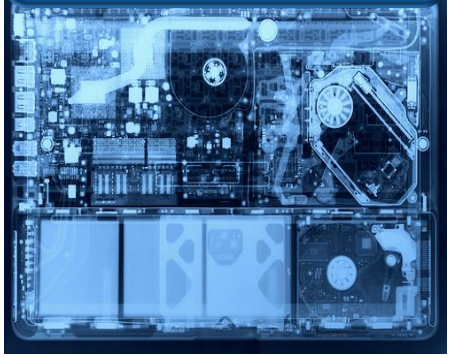
PASSPORT
A part of Experian

The key is leveraging a multi-layered approach

Identity

- Knowledge-based authentication
- Excessive permutations of identity information
- Identity associated with fraud

Device Trust & Compatibility



- History of device with user
- Configuration incompatible with user preferences
- Internal incompatibilities

Hostile Device Behavior

- Impersonate multiple identities
- Represent multiple identities while not being trusted by them
- Repeat infrequent activities (e.g. changing phone # or email)

Criminal History

- Device associated with confirmed fraud
- IP address associated with confirmed fraud
- Email address associated with confirmed fraud

Key Takeaways

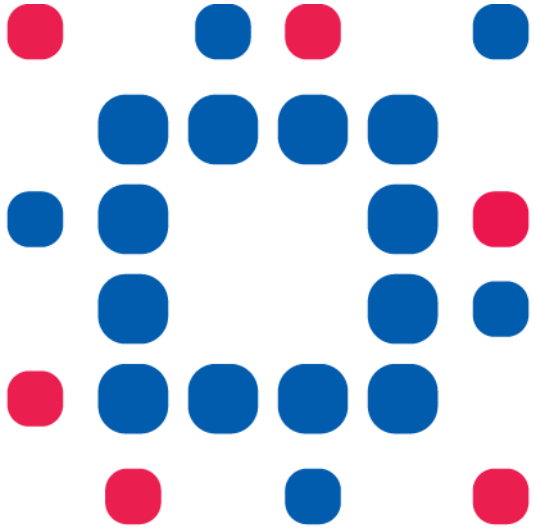
Be proactive. Deploy multiple prevention and detection controls.

- Deploy a multi-layer portal protection strategy
  - A password isn't enough
  - Encryption is a necessity, but not **the answer**
- Protect all portals with sensitive information
  - Attacks are not going to stop
- Monitor internal and external portal users
- Educate portal users on suspicious behaviors

PASSPORT
A part of Experian

Questions

Questions?



Experian®

A world of insight

Experian Health

PASSPORT
A part of Experian