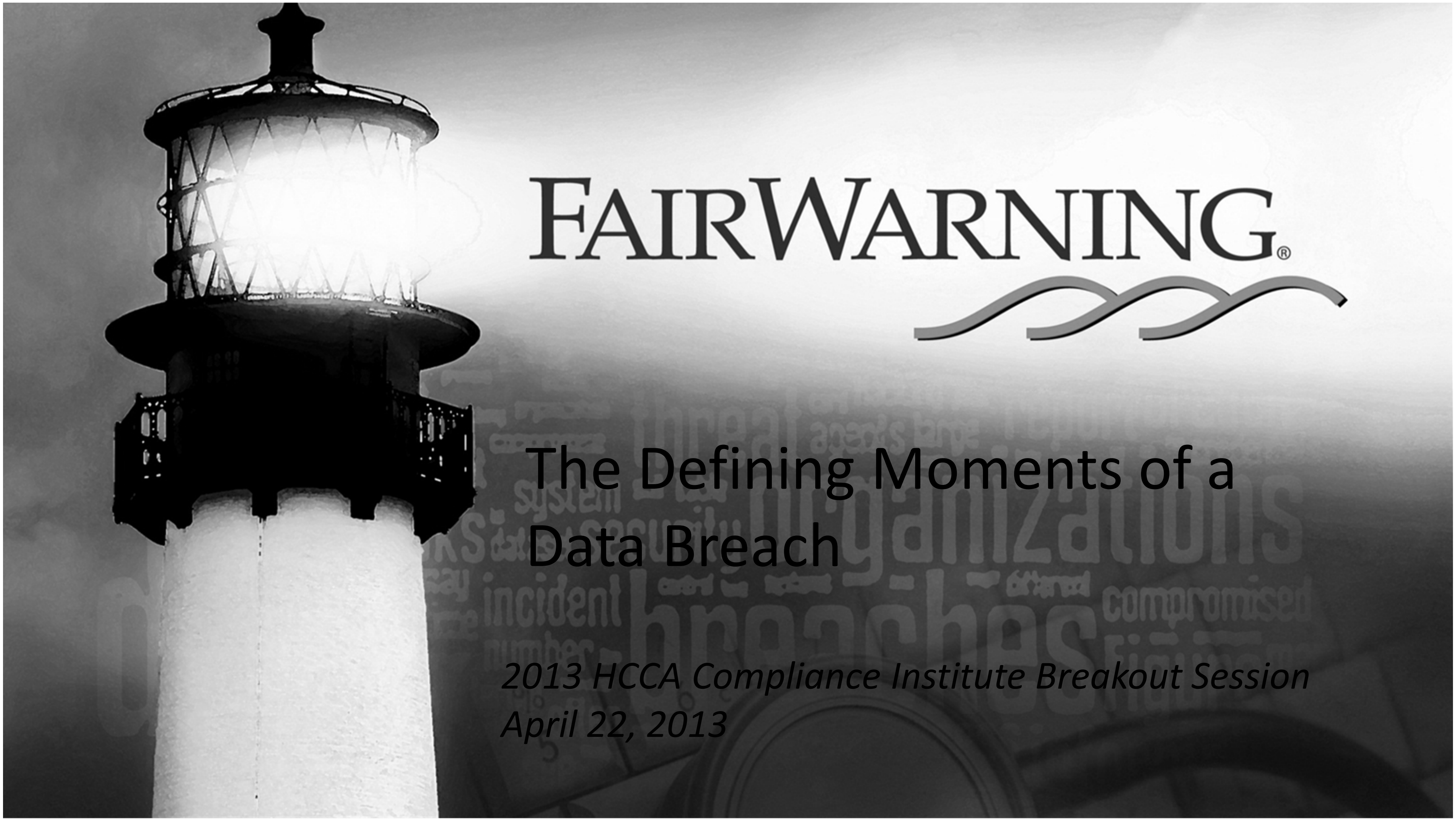


FairWarning®

The Defining Moments of a Data Breach

2013 HCCA Compliance Institute Breakout Session
April 22, 2013

Today’s Panel

John Ford

Sienna Group

John.ford@siennagrc.com

Kurt J. Long

FairWarning® Founder and CEO

Kurt@FairWarning.com

Introduction

- Data breaches in Healthcare organizations take on many forms from inadvertent losses such as lost laptops, or broken business processes to sophisticated fraud schemes that are enabled through the theft of patient and provider information
- Research shows that most organizations are not well prepared to detect and combat fraud as a result of a data breach, and the current model of “pay and chase” does not capture or recover all of the losses amassed in the current schemes

Patient & Physician Information: Fuel for Fraud

- Healthcare fraud in the U.S. costs the industry $80 billion to $225 billion per year
- Theft of patient and physician information is likely the biggest unchecked and unmeasured vulnerability plaguing the healthcare industry
- Government, payers and care providers must recognize that the next logical extension for consideration related to fraud prevention is to **catch criminal behavior at the point of origin**

Theft of Patient & Physician Information

Common Scenarios include utilizing patient information to/for:

- Bill for services not rendered
- Defraud Medicare, Medicaid or private payers
- Use of unnecessary medical supplies and equipment for the purpose of billing a third-party
- Over prescribe medication in return for cash payments or agreement to undergo additional medical procedures
- Falsify patient medical records with phantom results from procedures not performed, but billed to a third party
- Steal patients’ health benefits
- Pharmacy fraud – filling a patient’s prescription for a cheaper, similar or generic medication to the one that is prescribed, and billing insurance payers for the name-brand prescribed medication

Theft of Patient & Physician Information

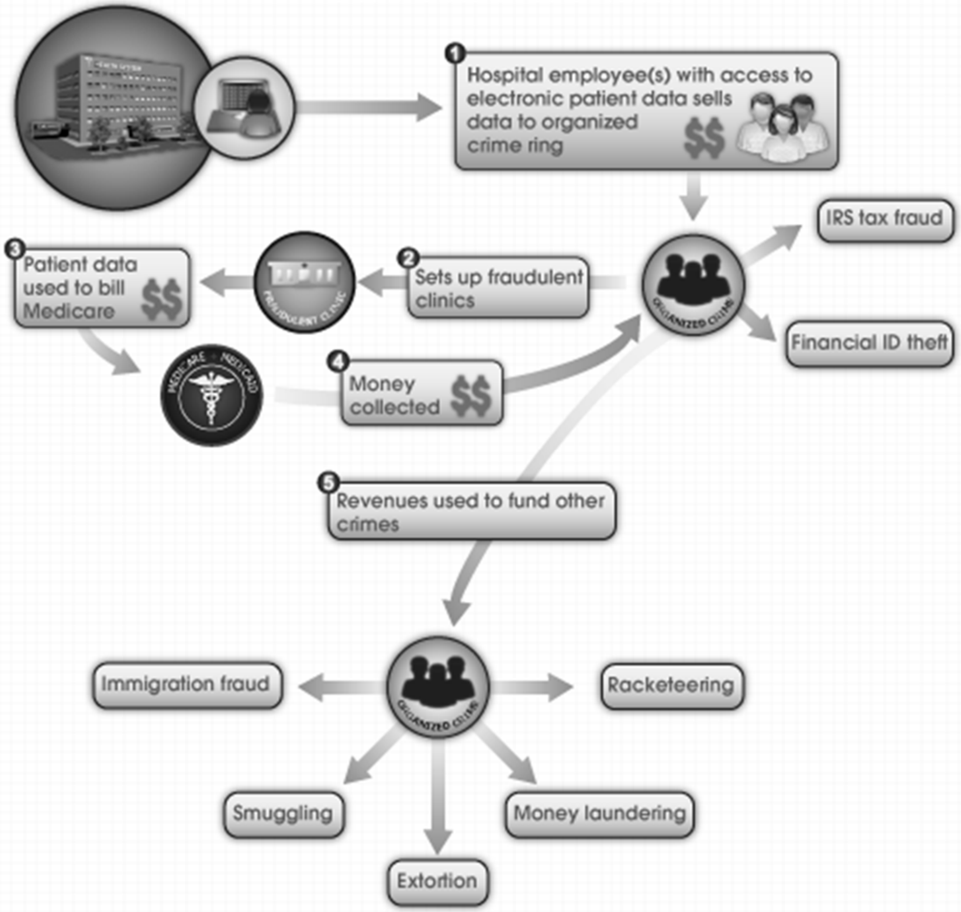
“Follow-on” crimes that fall out of use of stolen patient and physician data:

- IRS tax fraud – utilizing identifying patient information to file false tax returns on a grand scale
- Identity theft
- Racketeering
- Mail fraud
- Immigration fraud
- Creation of “shell” businesses for the purpose of money laundering as well as other methods of money laundering
- Using proceeds derived from fraud to fund illegal import / export businesses

Organized Crime & Healthcare Fraud

- Organized criminals have taken notice that care providers have critical privacy and security vulnerabilities.
- Examples:
  - Armenian crime ring
  - Russian crime scheme

Patient Data Fuels Fraud



1 Hospital employee(s) with access to electronic patient data sells data to organized crime ring

2 Sets up fraudulent clinics

3 Patient data used to bill Medicare

4 Money collected

5 Revenues used to fund other crimes

IRS tax fraud

Financial ID theft

Immigration fraud

Racketeering

Smuggling

Money laundering

Extortion

Defining Moment #1

- Organization is struggling for information:
  - Executive teams are mobilized
  - Operational teams are looking for clues
  - General theme is the development of a plan of action
- Defining Moment – Not having an Incident Response Plan that accounts for these scenarios

Defining Moment #2

- Upon notification the organization will be pressed for an explanation by the media, regulators, patients, and providers. Key issues they will need to address are:
  - How the internal data breach occurred
  - Why was it not detected
  - Understanding of the scope of fraud as a result of the breach
  - What patients and providers should be doing as a result of the breach
  - What the organization is doing as a result of the breach
- Defining Moment – Have a well-crafted communications plan that is delivered to the media by a communications expert

Defining Moment #3

- The impact to patients and providers is both lengthy and costly
- Healthcare organizations bear the reputational, and financial risks
- According to the “The Risk of Insider Fraud, Second Annual Study”, released by the Ponemon Institute in February 2013:
  - It takes an organization an average of 87 days to determine that insider fraud has occurred and 105 days to determine root cause
  - With only one-third of the cases being closed with actionable evidence the data implies that the organizations, as well as patients and providers are vulnerable to repeat offenses
- Defining Moment – Current methods for detecting and preventing breaches must include active user activity monitoring, and thorough log correlation and analysis

Current Fraud Prevention Strategies

- The “Pay and Chase” Model: CMS issues Medicare and Medicaid payments prior to validating claims. If and when the claim is deemed fraudulent or is not validated, CMS must “chase down” the repayment of funds
  - lends itself to waste of law enforcement hours, efforts and money associated with executing stings
- Strike Force: a coordinated team of federal, state and local law enforcement tasked to fight healthcare fraud
  - Strike team successes are exciting and dramatic but given the sheer size of the fraud epidemic in healthcare, their efforts have had a negligible impact on fraud reduction

Modern Strategies to Impede Fraud

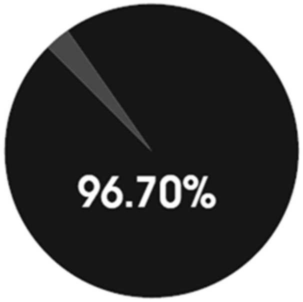
Future strategies must emphasize stopping fraud at the point of origin:

- CMS must work to produce better analytics to detect fraud earlier
- Government responsibility to conduct better vetting of care providers prior to payment
- “Pay and Chase Model” must be revamped
- Government mandated audit log trails for all applications touching PHI would arm privacy and security professionals with a powerful weapon in the fight against fraud, shining light on suspect transactions

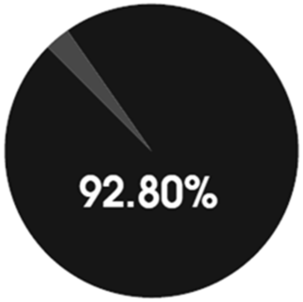
Independent Survey Findings

What Compliance, Privacy & Risk Professionals are Saying:

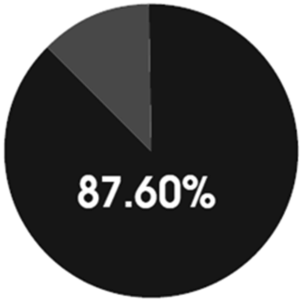
Nearly 9 out of 10 survey respondents are in favor of a government mandate on vendors of all healthcare applications that touch PHI requiring them to produce robust audit trails.



Respondents stating that robust audit trails from all applications that touch PHI would benefit them in **thwarting and detecting privacy breaches**



Respondents stating that robust audit trails would benefit their organization´s **anti-fraud programs**



Respondents **in favor of a government mandate** on vendors of all healthcare applications that touch PHI requiring them to produce robust audit logs

Conclusion

- This presentation was intended to leave you with the following key points:
  - Healthcare organizations have unique vulnerabilities to data breaches and fraud given the predominance of sensitive data, and wide-spread access to support care-providing functions
  - Crime rings are mature and prey on open vulnerabilities of organizations with the intent of committing fraud
  - Current “pay and chase” model is inefficient and does little to capture the accuracy of the issue
  - Healthcare organizations need to increase their efforts in monitoring user-activity for inappropriate use in an effort to reduce the time it takes to detect data breaches and potential fraud

Questions & Answers

Contact Information

John Ford

Sienna Group

John.ford@siennagrc.com

Kurt J. Long

FairWarning® Founder and CEO

Kurt@FairWarning.com