The 25th National HIPAA Summit

Introduction

Adam H. Greene, JD, MPH
Davis Wright Tremaine LLP

September 15, 2016

Morning Agenda

- Introduction and Overview (8:00 am to 8:30 am)

- OCR Policy and Implementation Update (8:30 am to 10:00 am)

- Break (10:00 am to 10:30 am)

- Best Practices in Preparing for and Responding to OCR Desk and Onsite Audits (10:30 am to 11:30 am)

- Keynote: FTC Role in Healthcare Privacy and Security (11:30 am to 12:00 pm)

- Networking Luncheon (12:00 pm to 1:00 pm)

Housekeeping

New Challenges

Hey Pokemon Go Players. Have extra lures? Then drive to your nearest Children's Hospital and drop the lure there. There are plenty of kids who would love to go out and collect Pokemon, but they are stuck in bed, so this will help them.

Team Valor
@PoGoTeamValor

Follow

If you happen to live near or work at a children's hospital be kind and drop a lure. ❤ #TeamValor #PokemonGo
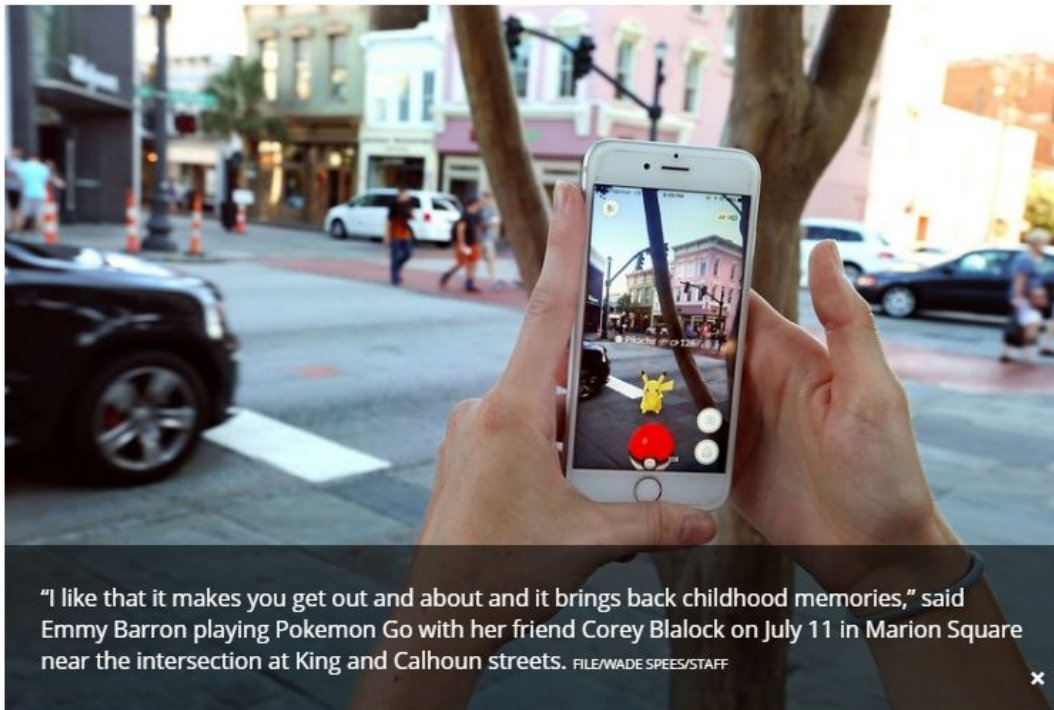
1:10 PM - 15 Jul 2016

Hospital bans 'Pokemon Go' from campus citing patient safety, privacy

Lauren Sausser ✉ Email 🐦 @laurenmsausser

Jul 20 2016 12:31 pm 🕐 Jul 20 12:45 pm

"I like that it makes you get out and about and it brings back childhood memories," said Emmy Barron playing Pokemon Go with her friend Corey Blalock on July 11 in Marion Square near the intersection at King and Calhoun streets. FILE/WADE SPEES/STAFF

Most Popular

Concern for Southeast rises as storm approaches the Caribbean

$31.8 million Coastal Carolina stadium project approved

Deputies: South Carolina mom killed newborn by putting him in refrigerator

No dead manatee found during search sparked by report

At least one South Carolina hospital is working with the creators of "Pokemon Go" to disable the game on campus and inside its buildings.

JOHNS HOPKINS
MEDICINE

Search

ABOUT   **HEALTH**   **PATIENT CARE**   **RESEARCH**   **EDUCATION**

News and Publications

< View All Publications

Pokemon Go' Craze Helps Pediatric Patients Feel Like Regular Kids

Even while in the hospital, patients "gotta catch 'em all"

Date: 08/09/2016

In the second-floor lobby of the Johns Hopkins Children's Center, 19-year-old Brianna Boyd makes her way past the suspended yellow pufferfish display, head down and eyes cast on the iPhone in her hand. While she may appear to be another smartphone-absorbed teenager, she is actually focused on a game that helped her recover from surgery just a week prior.

New Challenges

- What is your photography policy for patients?

- What is your policy on facility visitors in public areas? In non-public areas?

- Can workforce install apps on work phones?

- Can workforce use personal devices at the facility?

New Enforcement

Enforcement Highlights

38 OCR Settlements

2 Civil Monetary Penalty Actions

$52,589,700

In settlements and CMPs

$1,264,471

Average settlement amount

27 of **40**

enforcement actions arose from breach reports to HHS

40

5 Required an internal monitor

4 Required an external monitor

9 **Monitor required in 9 out of 40**

Enforcement Highlights

1	1	2	3	5	5	7	6	10
in 2008	in 2009	in 2010	in 2011	in 2012	in 2013	in 2014	in 2015	in 2016
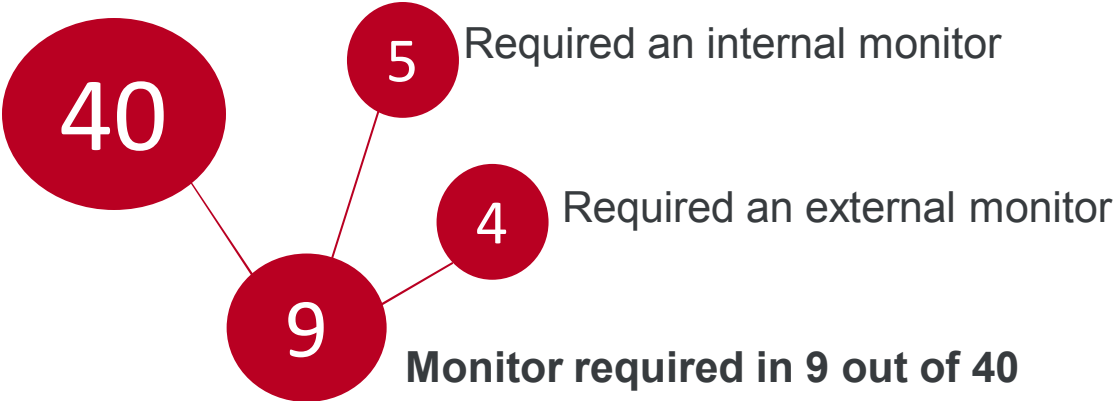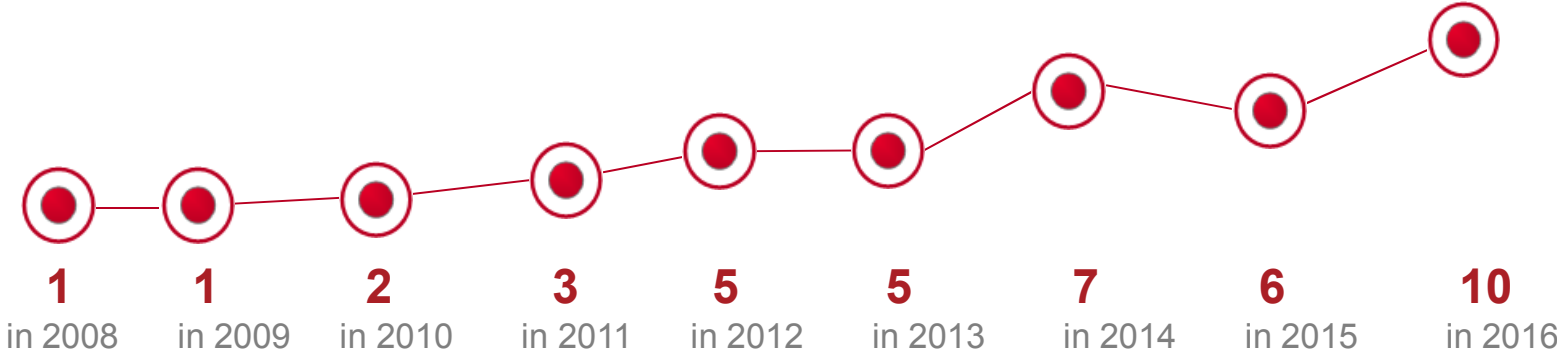
(as of August 23, 2016)

Average minimum length of a corrective plan:

APPROXIMATELY 2 YEARS

Average attorney general enforcement action:

$347,909*

*may represent financial settlements associated with claims unrelated to HIPAA violations
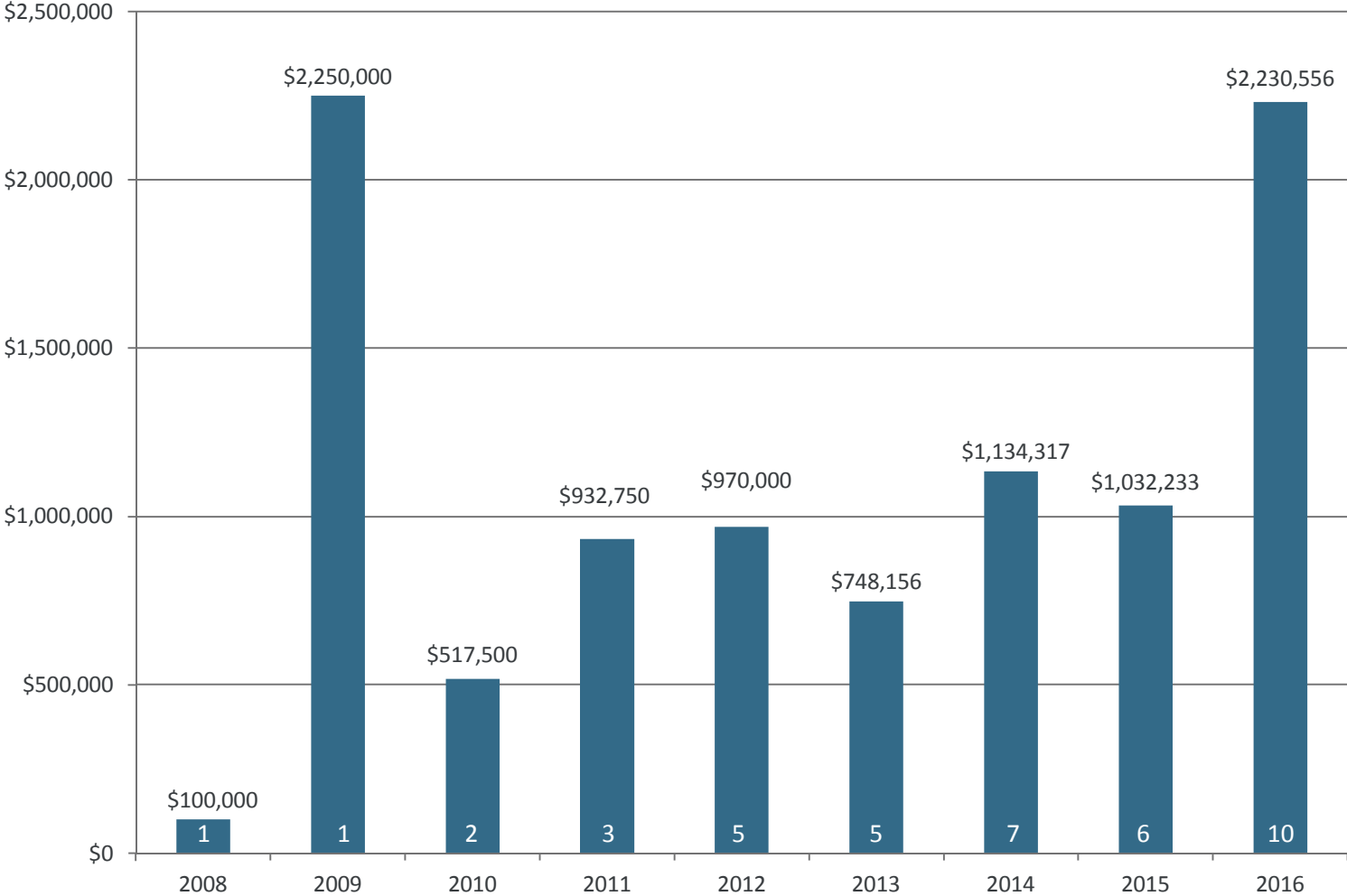
11 actions by state attorneys general/ in just **over 6 years**:

5	1	1
Massachusetts	New York	Vermont
2	1	1
Connecticut	Indiana	Minnesota

Average Settlement Amount

New Case Law

Syllabus

To establish injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."

SPOKEO, INC. v. ROBINS

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

We take no position as to whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact— was correct.

imposes liability on "[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any" individual, §1681n(a).

Petitioner Spokeo, Inc., an alleged consumer reporting agency, operates a "people search engine," which searches a wide spectrum of

We conclude that the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n).

OPINION OF THE COMMISSION

By Chairwoman Edith Ramirez, for the Commission:

This case concerns the alleged failure by Respondent LabMD, Inc. to protect the sensitive personal information, including medical information, of consumers whose physicians had entrusted that information to the company. Specifically, Complaint Counsel alleges that LabMD failed to implement reasonable security measures to protect the sensitive consumer information on its computer network and therefore that its data security practices were unfair under Section 5 of the Federal Trade Commission Act. The Administrative Law Judge dismissed the Complaint following an administrative trial, holding that Complaint Counsel had not shown that LabMD's data security practices either caused or were likely to cause substantial injury.

As we explain below, we conclude that the ALJ applied the wrong legal standard for

New [?] Security Threats

New [?] Security Threats

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and **availability**.

Source: NIST Glossary of Key Information Security Terms

Privacy & Security

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By **Bill Siwicki** | May 23, 2016 | 02:58 PM

IEEE computer society

The Community for Technology Leaders

◆IEEE

CSDL   Institutions and Libraries   About   Resources ▾

Search the CSDL   Subscribe   Login

Cryptovirology: Extortion-Based Security Threats and Countermeasures

Oakland, Ca
May 6, 1996 to May 8, 1996
ISBN: 0-8186-7417-2
pp: 0129

Adam Young

Moti Yung

DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/SECPRI.1996.502676

FULL ARTICLE

📄 PDF

🛒 BUY

📶 RSS Feed

Ⓢ SUBSCRIBE

CITATION ▾

SHARE ▾

ABSTRACT

Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. In this paper we present the idea of ``Cryptovirology'' which employs a twist on cryptography, showing that it can also be used offensively. By being offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents. In this paper we analyze potential threats and attacks that rogue use of cryptography can cause when combined with rogue software (viruses, Trojan horses), and demonstrate them experimentally by presenting an implementation of a ``cryptovirus'' that we have tested (we took careful precautions in the process to insure that the virus remained contained). Public-key cryptography is essential to the attacks that we demonstrate (which we call "cryptovirological attacks"). We also suggest countermeasures and mechanisms to cope with and prevent such attacks. These attacks have implications on how the use of cryptographic tools should be managed and audited in general purpose computing environments, and imply that access to cryptographic tools should be well controlled. The experimental virus demonstrates how cryptographic packages can be condensed into a small space, which may have independent applications (e.g., cryptographic module design in small mobile devices).

SEARCH

Articles by Adam Young

Articles by Moti Yung

CITATION

2016 CS Election

Cheer Up