Illegal HIPAA Complaint Retaliation by LSUHealthNewOrleans

First HIPAA Violation by LSUHealthNewOrleans

On June 17, 2014, I reported an apparent HIPAA violation to LSUHealthNewOrleans. They did not reply to me at all, but took down the server that was exposing patient data.

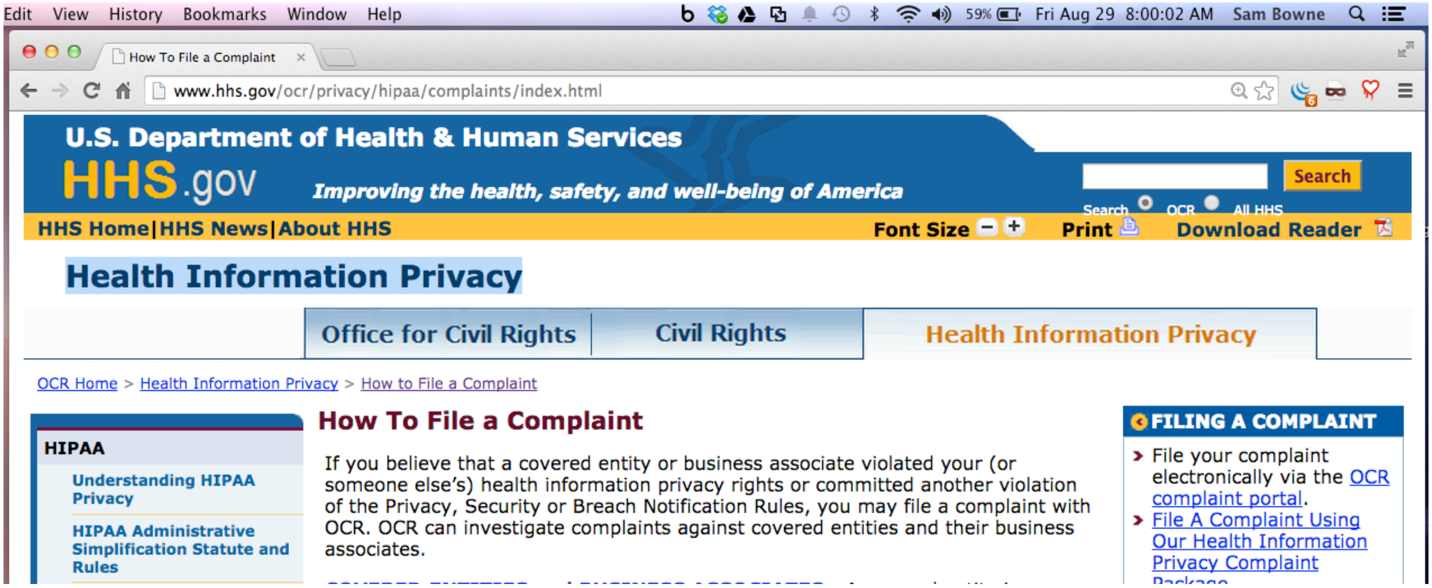
This is the email I sent:

> **Sam Bowne <sam.bowne@gmail.com>**
> **to: webmaster@lsuhsc.edu,**
> **nocompliance@lsuhsc.edu,**
> **lhholl@lsuhsc.edu**
> **date: Tue, Jun 17, 2014 at 11:45 AM**
> **subject: Exposed patient data on public server**
> **mailed-by: gmail.com**
>
> **Hello:**
>
> **I am Sam Bowne, an instructor at City College San Francisco, and I found two security problems on your server with a Google search.**
>
> **Your FTP server has been compromised, and some files named "w0000000t" were added to it.**
>
> **However, that's very minor compared to the fact that you have dozens of files publicly exposed on that server containing medical data about thousands of patients.**
>
> **Here's the server root:**
>
> **ftp://conway.lsuhsc.edu/**
>
> **Here's an example file showing approximately 2000 of what appear to be patient names:**
>
> **ftp://conway.lsuhsc.edu/EACHBSTMRP20121120.txt**
>
> **Here are some patient addresses:**
>
> **ftp://conway.lsuhsc.edu/EACHB20121122.txt**
>
> **There are many more files there--you may have a serious violation of HIPAA regulations here.**
>
> **These files have apparently been exposed for at least a year, and have already been copied to other servers by FTP search engines:**
>
> **http://filemare.com/en-us/browse/155.58.160.62@@@60/12**
>
> **The "w0000000t" file is apparently part of a mass compromise of Microsoft FTP servers, which was found but not explained by a French security company named QuarkLabs in this slide:**
>
> **http://samsclass.info/lulz/w00t-ftp.png**
>
> **Full presentation here:**
>
> **http://www.quarkslab.com/dl/D2T1-Why-Port-Scans-are-for-Pussies.pdf**
>
> **Please alert your technical and legal staff.**
>
> **I am happy to answer any questions you may have.**
>
> **Sam Bowne sbowne@ccsf.edu**

Illegal Retaliation by LSUHealthNewOrleans

On August 19 and 20, false news reports appeared accusing an unnamed "computer science professor from the City College of San Francisco" of hacking into their server during a classroom demonstration. I never hacked anything, and I did not demonstrate anything in any class--I was not teaching any classes on June 17, because it was during Summer vacation.

Apparently the HIPAA compliance office at LSUHealthNewOrleans took retaliation against me, by inventing this wholly false accusation and passing it on to the press. Such retaliation is forbidden under HIPAA. Here are the relevant portions of the hhs.gov website, and some articles about the laws forbidding retaliation:


Edit View History Bookmarks Window Help
59% Fri Aug 29 8:00:02 AM Sam Bowne
How To File a Complaint
www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search OCR All HHS
HHS Home|HHS News|About HHS
Font Size − +
Print
Download Reader
Office for Civil Rights
Civil Rights
Health Information Privacy
OCR Home > Health Information Privacy > How to File a Complaint
HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules

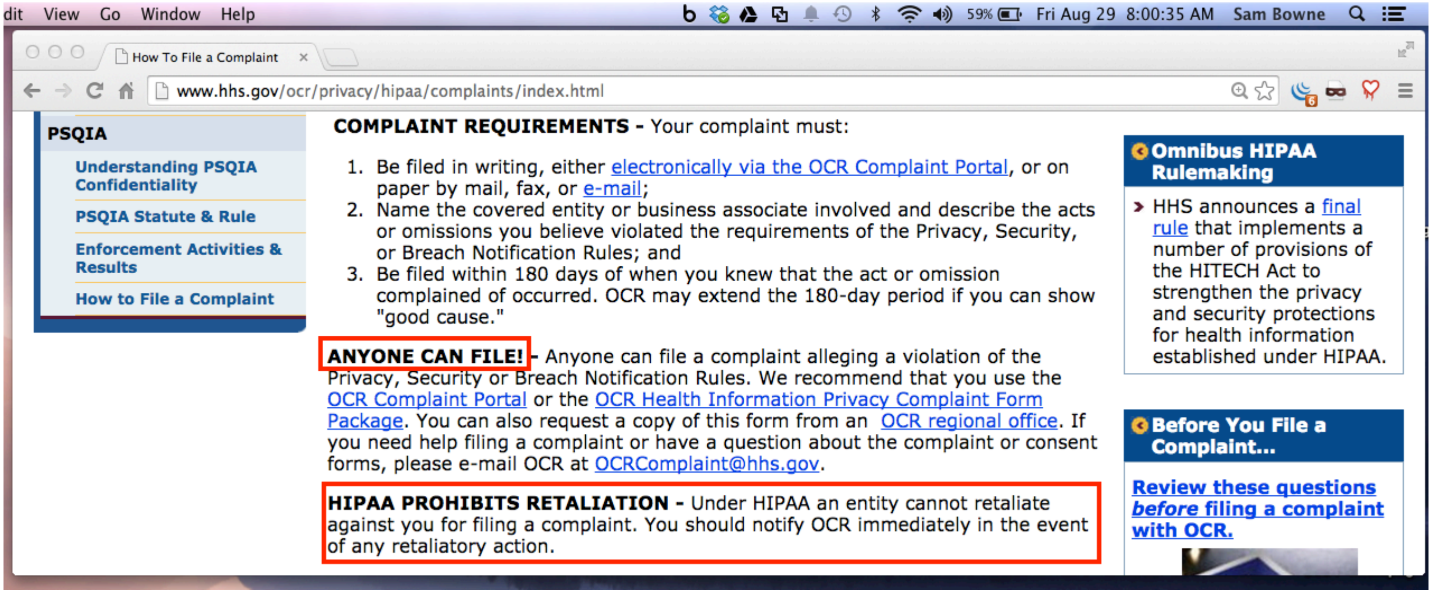
Health Information Privacy

How To File a Complaint

If you believe that a covered entity or business associate violated your (or someone else's) health information privacy rights or committed another violation of the Privacy, Security or Breach Notification Rules, you may file a complaint with OCR. OCR can investigate complaints against covered entities and their business associates.

FILING A COMPLAINT

- File your complaint electronically via the OCR complaint portal.
- File A Complaint Using Our Health Information Privacy Complaint Package


dit View Go Window Help
59% Fri Aug 29 8:00:35 AM Sam Bowne
How To File a Complaint
www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
PSQIA
Understanding PSQIA Confidentiality
PSQIA Statute & Rule
Enforcement Activities & Results
How to File a Complaint

COMPLAINT REQUIREMENTS - Your complaint must:

1. Be filed in writing, either electronically via the OCR Complaint Portal, or on paper by mail, fax, or e-mail;
2. Name the covered entity or business associate involved and describe the acts or omissions you believe violated the requirements of the Privacy, Security, or Breach Notification Rules; and
3. Be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause."

ANYONE CAN FILE! - Anyone can file a complaint alleging a violation of the Privacy, Security or Breach Notification Rules. We recommend that you use the OCR Complaint Portal or the OCR Health Information Privacy Complaint Form Package. You can also request a copy of this form from an OCR regional office. If you need help filing a complaint or have a question about the complaint or consent forms, please e-mail OCR at OCRComplaint@hhs.gov.

HIPAA PROHIBITS RETALIATION - Under HIPAA an entity cannot retaliate against you for filing a complaint. You should notify OCR immediately in the event of any retaliatory action.

Omnibus HIPAA Rulemaking

- HHS announces a final rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA.

Before You File a Complaint...

Review these questions before filing a complaint with OCR.

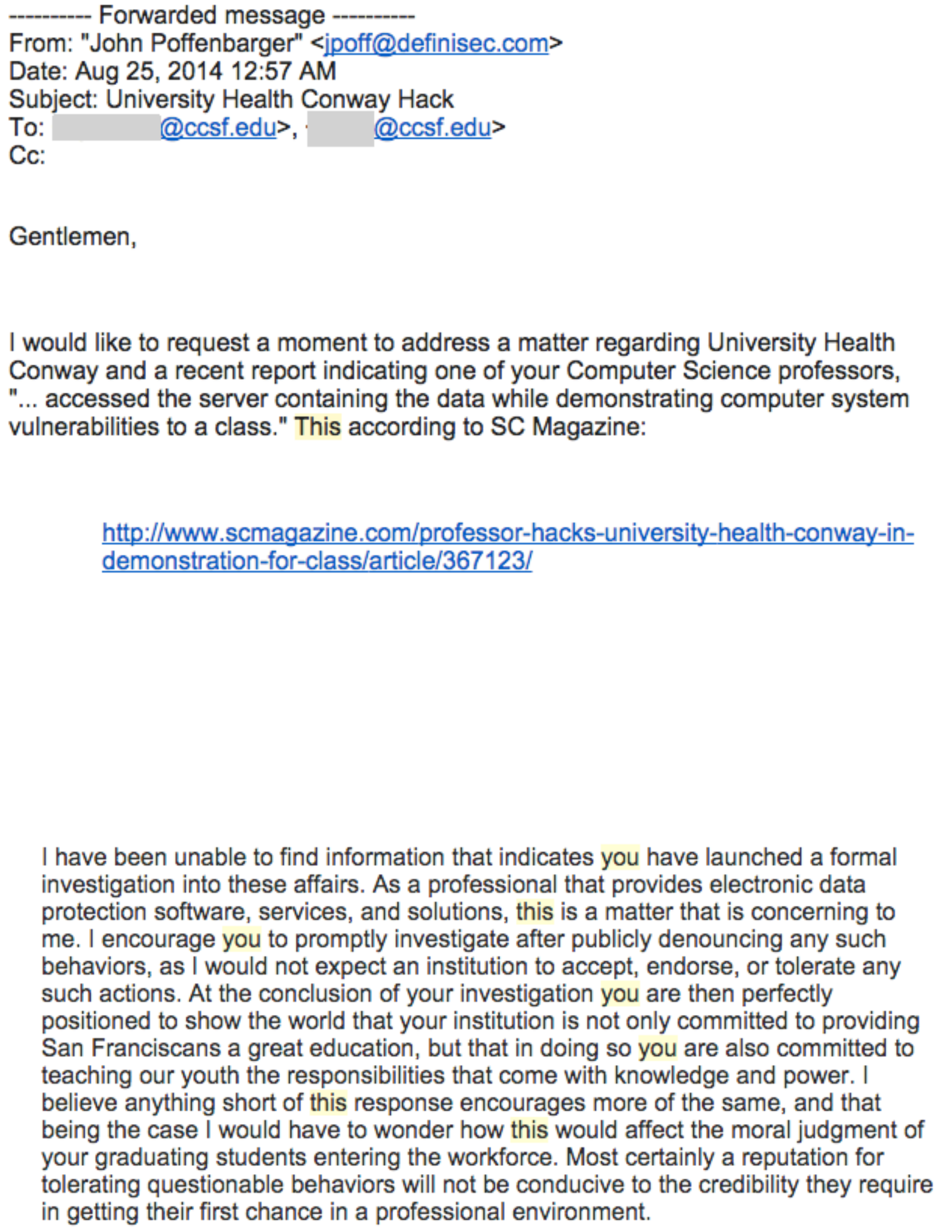
[HHS.GOV: Health Information Privacy]

[What does HIPAA say about a covered entity retaliating against an employee or others who file complaints or otherwise exercise their rights under HIPAA? (2004)]

[HIPAA Whistleblower Protections Promote Information Governance (2014)]

Letter from Definitive Data Security, Inc.

I became aware of this on August 28, because of this letter sent to computer science administrators at City College San Francisco:



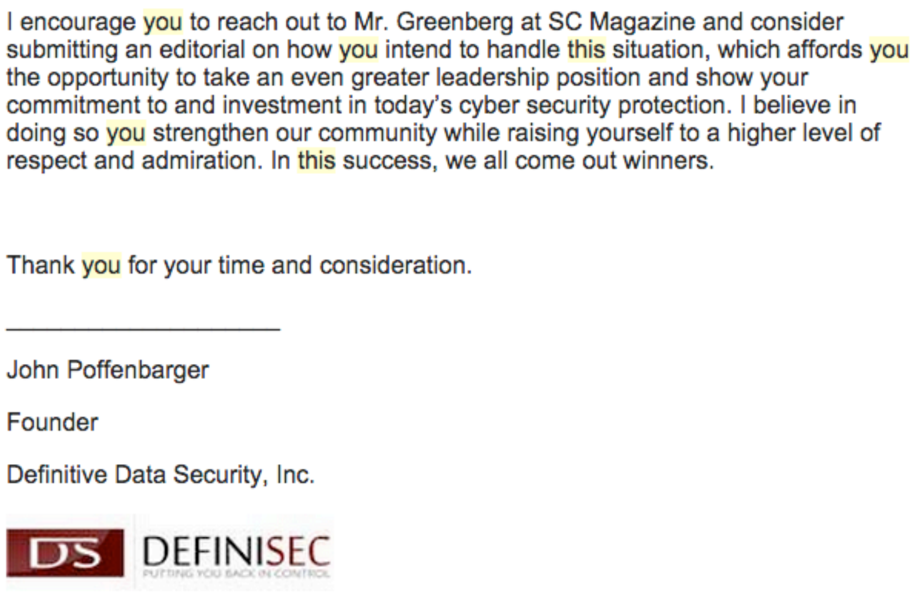
---------- Forwarded message ----------
From: "John Poffenbarger" <jpoff@definisec.com>
Date: Aug 25, 2014 12:57 AM
Subject: University Health Conway Hack
To: [redacted]@ccsf.edu>, [redacted]@ccsf.edu>
Cc:

Gentlemen,

I would like to request a moment to address a matter regarding University Health Conway and a recent report indicating one of your Computer Science professors, "... accessed the server containing the data while demonstrating computer system vulnerabilities to a class." This according to SC Magazine:

http://www.scmagazine.com/professor-hacks-university-health-conway-in-demonstration-for-class/article/367123/

I have been unable to find information that indicates you have launched a formal investigation into these affairs. As a professional that provides electronic data protection software, services, and solutions, this is a matter that is concerning to me. I encourage you to promptly investigate after publicly denouncing any such behaviors, as I would not expect an institution to accept, endorse, or tolerate any such actions. At the conclusion of your investigation you are then perfectly positioned to show the world that your institution is not only committed to providing San Franciscans a great education, but that in doing so you are also committed to teaching our youth the responsibilities that come with knowledge and power. I believe anything short of this response encourages more of the same, and that being the case I would have to wonder how this would affect the moral judgment of your graduating students entering the workforce. Most certainly a reputation for tolerating questionable behaviors will not be conducive to the credibility they require in getting their first chance in a professional environment.



I encourage you to reach out to Mr. Greenberg at SC Magazine and consider submitting an editorial on how you intend to handle this situation, which affords you the opportunity to take an even greater leadership position and show your commitment to and investment in today's cyber security protection. I believe in doing so you strengthen our community while raising yourself to a higher level of respect and admiration. In this success, we all come out winners.

Thank you for your time and consideration.

____

John Poffenbarger

Founder

Definitive Data Security, Inc.

DS DEFINISEC

PUTTING YOU BACK IN CONTROL

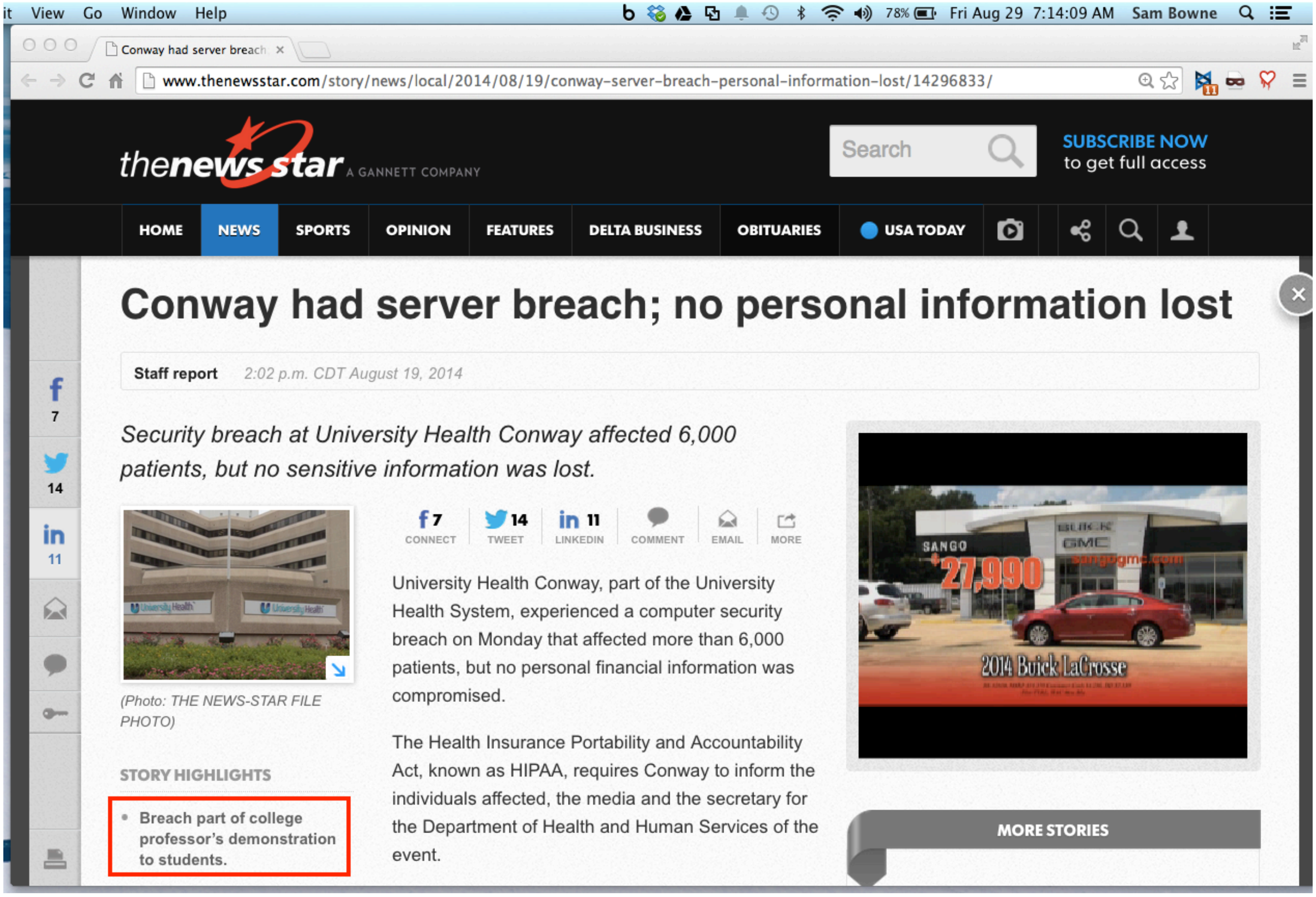
It is not clear how Definitive Data Security is involved here; they may merely be gullible enough to believe lies they read in the media.

Lies Published by Gannett Media

Here is the original lying news report from "thenews star, A GANNETT COMPANY":

Conway had server breach; no personal information lost

Here are two excerpts from that article, with the relevant passages outlined in red:



it View Go Window Help
78% Fri Aug 29 7:14:09 AM Sam Bowne
Conway had server breach ×
www.thenewsstar.com/story/news/local/2014/08/19/conway-server-breach-personal-information-lost/14296833/
thenewsstar A GANNETT COMPANY
Search
SUBSCRIBE NOW to get full access
HOME NEWS SPORTS OPINION FEATURES DELTA BUSINESS OBITUARIES USA TODAY
f 7 CONNECT
14 TWEET
in 11 LINKEDIN
COMMENT
EMAIL
MORE
SANGO $27,990 BUICK GMC sangogmc.com 2014 Buick LaCrosse
MORE STORIES

Conway had server breach; no personal information lost

Staff report *2:02 p.m. CDT August 19, 2014*

Security breach at University Health Conway affected 6,000 patients, but no sensitive information was lost.

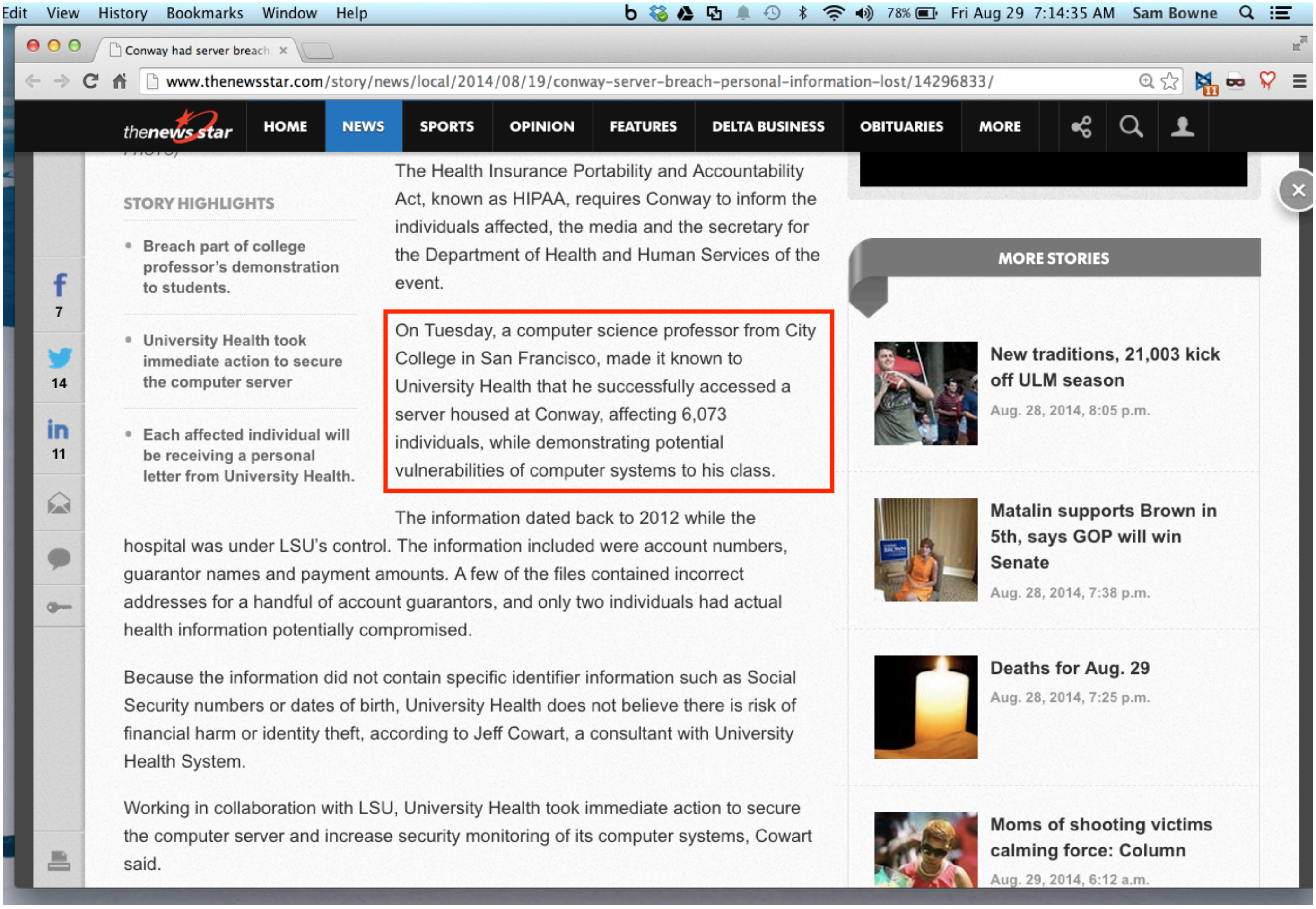
(Photo: THE NEWS-STAR FILE PHOTO)

STORY HIGHLIGHTS

- **Breach part of college professor's demonstration to students.**

University Health Conway, part of the University Health System, experienced a computer security breach on Monday that affected more than 6,000 patients, but no personal financial information was compromised.

The Health Insurance Portability and Accountability Act, known as HIPAA, requires Conway to inform the individuals affected, the media and the secretary for the Department of Health and Human Services of the event.


Edit View History Bookmarks Window Help
78% Fri Aug 29 7:14:35 AM Sam Bowne
Conway had server breach ×
www.thenewsstar.com/story/news/local/2014/08/19/conway-server-breach-personal-information-lost/14296833/
thenewsstar
HOME
NEWS
SPORTS
OPINION
FEATURES
DELTA BUSINESS
OBITUARIES
MORE
f 7
14
in 11

STORY HIGHLIGHTS

- Breach part of college professor's demonstration to students.
- University Health took immediate action to secure the computer server
- Each affected individual will be receiving a personal letter from University Health.

The Health Insurance Portability and Accountability Act, known as HIPAA, requires Conway to inform the individuals affected, the media and the secretary for the Department of Health and Human Services of the event.

On Tuesday, a computer science professor from City College in San Francisco, made it known to University Health that he successfully accessed a server housed at Conway, affecting 6,073 individuals, while demonstrating potential vulnerabilities of computer systems to his class.

The information dated back to 2012 while the hospital was under LSU's control. The information included were account numbers, guarantor names and payment amounts. A few of the files contained incorrect addresses for a handful of account guarantors, and only two individuals had actual health information potentially compromised.

Because the information did not contain specific identifier information such as Social Security numbers or dates of birth, University Health does not believe there is risk of financial harm or identity theft, according to Jeff Cowart, a consultant with University Health System.

Working in collaboration with LSU, University Health took immediate action to secure the computer server and increase security monitoring of its computer systems, Cowart said.

MORE STORIES

New traditions, 21,003 kick off ULM season
Aug. 28, 2014, 8:05 p.m.

Matalin supports Brown in 5th, says GOP will win Senate
Aug. 28, 2014, 7:38 p.m.

Deaths for Aug. 29
Aug. 28, 2014, 7:25 p.m.

Moms of shooting victims calming force: Column
Aug. 29, 2014, 6:12 a.m.

Here are the specific lies I noticed in that article:

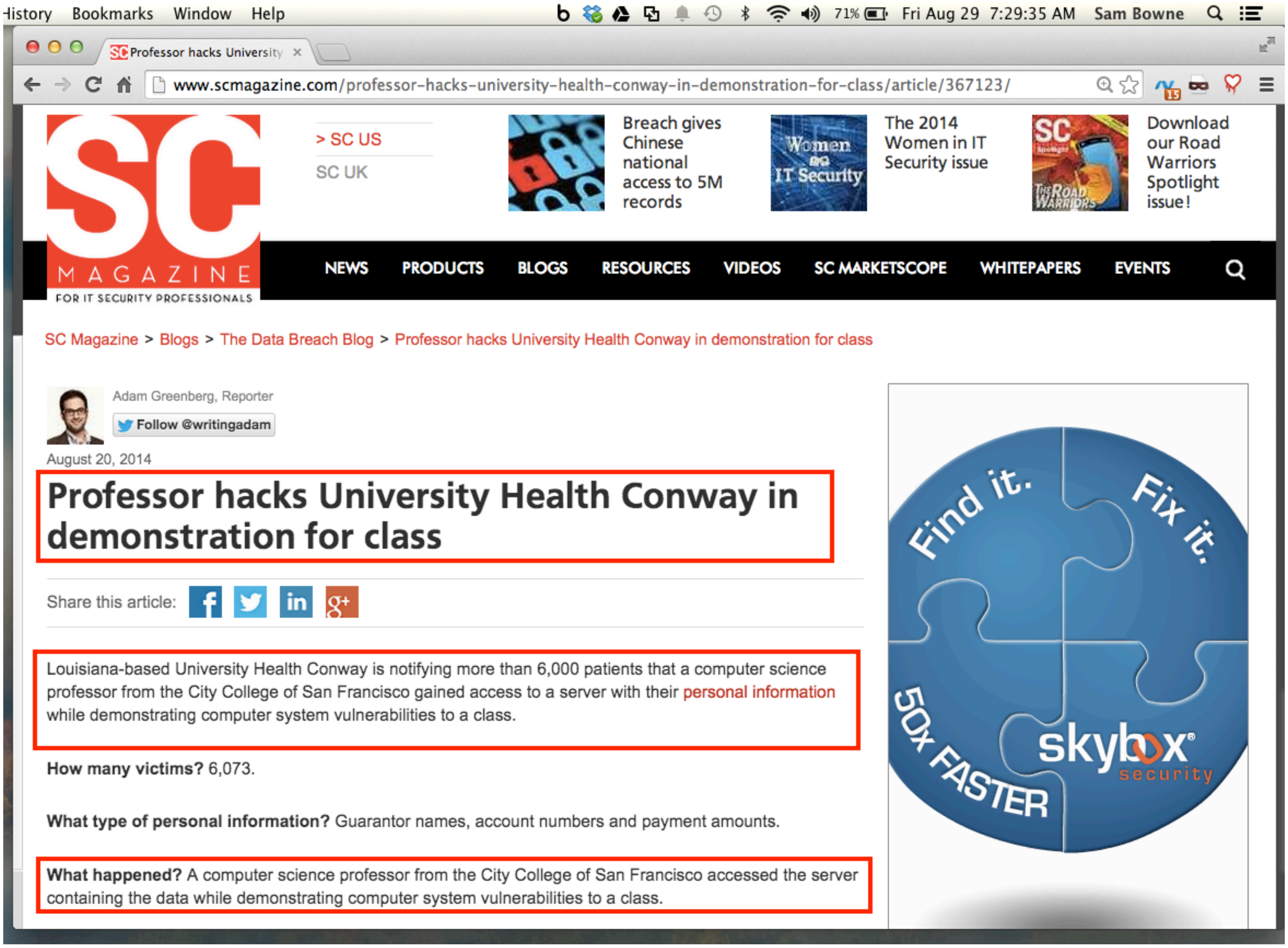
- This was not a classroom demonstration--I was not teaching any classes at this time.
- My notification did not occur on "Tuesday" in the week of August 19, 2014--it was sent on June 17, 2014.
- Describing this as a "breach" and saying I "successfully accessed a server" implies that I defeated some security measure to hack into a server. All I did was click on a link found by Google, and then click on the links on the FTP page. I did not "breach" anything.

Lies Published by Haymarket Media

Here is the lying article published on August 20, 2014 by SC Magazine, part of Haymarket Media:

Professor hacks University Health Conway in demonstration for class

Here are screen images of that article, with the relevant portions outlined in red:


History Bookmarks Window Help
71% Fri Aug 29 7:29:35 AM Sam Bowne
Professor hacks University
www.scmagazine.com/professor-hacks-university-health-conway-in-demonstration-for-class/article/367123/
SC MAGAZINE FOR IT SECURITY PROFESSIONALS
> SC US
SC UK
Breach gives Chinese national access to 5M records
The 2014 Women in IT Security issue
Download our Road Warriors Spotlight issue!
NEWS PRODUCTS BLOGS RESOURCES VIDEOS SC MARKETSCOPE WHITEPAPERS EVENTS
Find it. Fix it.
50x FASTER
skybox security

SC Magazine > Blogs > The Data Breach Blog > Professor hacks University Health Conway in demonstration for class

Adam Greenberg, Reporter

Follow @writingadam

August 20, 2014

Professor hacks University Health Conway in demonstration for class

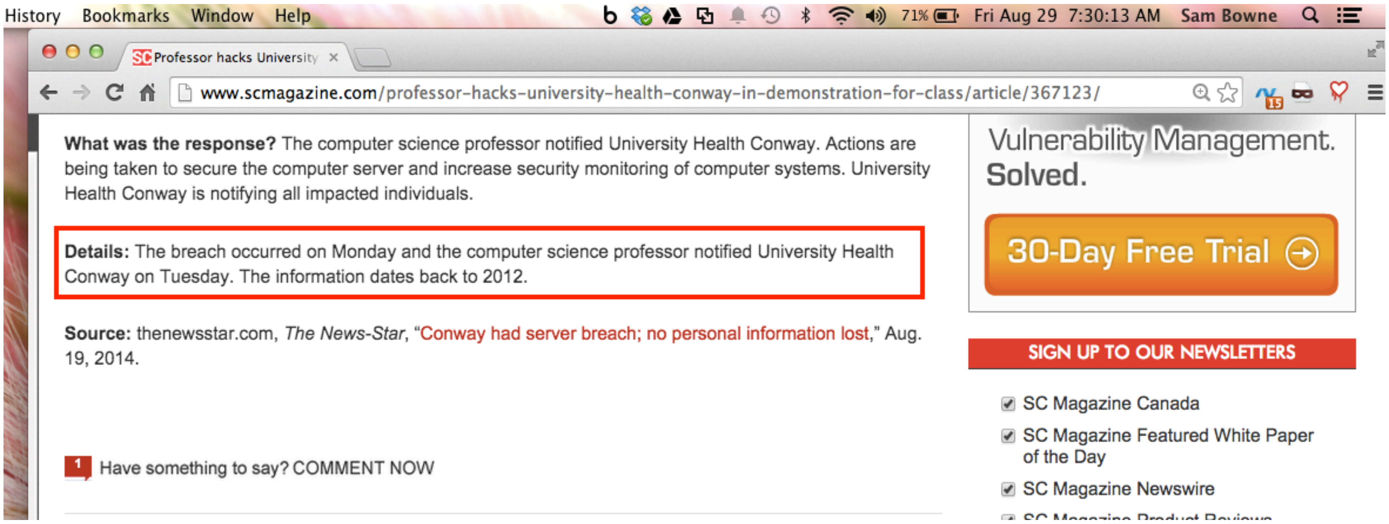
Share this article:

Louisiana-based University Health Conway is notifying more than 6,000 patients that a computer science professor from the City College of San Francisco gained access to a server with their personal information while demonstrating computer system vulnerabilities to a class.

How many victims? 6,073.

What type of personal information? Guarantor names, account numbers and payment amounts.

What happened? A computer science professor from the City College of San Francisco accessed the server containing the data while demonstrating computer system vulnerabilities to a class.


History Bookmarks Window Help
71% Fri Aug 29 7:30:13 AM Sam Bowne
Professor hacks University
www.scmagazine.com/professor-hacks-university-health-conway-in-demonstration-for-class/article/367123/
Vulnerability Management. Solved.
30-Day Free Trial
SIGN UP TO OUR NEWSLETTERS
SC Magazine Canada
SC Magazine Featured White Paper of the Day
SC Magazine Newswire

What was the response? The computer science professor notified University Health Conway. Actions are being taken to secure the computer server and increase security monitoring of computer systems. University Health Conway is notifying all impacted individuals.

Details: The breach occurred on Monday and the computer science professor notified University Health Conway on Tuesday. The information dates back to 2012.

Source: thenewsstar.com, *The News-Star*, "Conway had server breach; no personal information lost," Aug. 19, 2014.

1 Have something to say? COMMENT NOW

Extrapolating from the false report published by Gannett, Haymarket Media now explicitly accuses the professor of "hacking" into a server.

This article also falsely states that the breach occurrred on "Monday", apparently during the week of August 20, 2014. In fact, the patient data had been left exposed to the Internet for more than a year, and had been copied to other servers, as detailed in my original HIPAA violation report to LSUHealthNewOrleans.

My Demands

Personally, I demand public apologies and retractions from Gannett and Haymarket Media, and a public apology from LSUHealthNewOrleans.

However, I think LSUHealthNewOrleans now has larger problems: they appear to have acted in bad faith, inventing and spreading a false story to the media in retaliation for a HIPAA violation report. I imagine Federal regulators may require a bit more from them now than a mere apology.

Why This is an Open Letter

It is abundantly clear that LSUHealthNewOrleans, Gannett, and Haymarket Media care nothing for the truth, and that private messages sent to LSUHealthNewOrleans turn into fantastic malicious lies in the media, so it makes no sense to do any of this privately.

Since all those actors lack honesty, decency, and good faith, I decided to post everything pubicly, and to address high officials who might show some responsibility.

Published 8-29-14 by Sam Bowne