LILY HAY NEWMAN SECURITY 10.03.17 05:22 PM

6 FRESH HORRORS FROM THE EQUIFAX CEO'S CONGRESSIONAL HEARING

THE INITIAL DRAMA over Equifax's September data breach has mostly subsided, but the actual damage will play out for years. And indeed, there turns out to be plenty of spectacle and public controversy left. It was all on display at a Tuesday Congressional hearing, in which lawmakers questioned Equifax's former CEO Richard Smith in an attempt to make sense of how things went so wrong.

Before delving into the hearing itself—which went poorly enough—it's worth mentioning that it was bracketed by further unfortunate Equifax revelations. The company announced Monday that the total number of people impacted by its breach is not 143 million—the amount it first disclosed—but in fact 145.5 million. Its ability

dollar fraud-prevention contract last week.

And there's a lot more where that came from. Here are six important (and astonishing, disappointing, you name it) tidbits that came out of Tuesday's hearing.

1. The timeline of when executives knew what about the breach is both disheartening and suspect. Equifax has previously said that it was breached on May 13 and that it first discovered the problem on July 29. The company notified the public on September 7. But during Tuesday's hearing, former CEO Smith added that he first heard about "suspicious activity" in a customer-dispute portal, where Equifax tracks customer complaints and efforts to correct mistakes in their credit reports, on July 31. He moved to hire cybersecurity experts from the law firm King & Spalding to start investigating the issue on August 2. Smith claimed that, at that time, there was no indication that any customer's personally identifying information had been compromised. As it turns out, after repeated questions from lawmakers, Smith admitted he never asked at the time whether PII being affected was even a possibility.

Smith further testified that he didn't ask for a briefing about the "suspicious activity" until August 15, almost two weeks after the special investigation began and 18 days after the initial red flag. He received the briefing from King & Spalding and other forensic investigators on August 17. At that point, he said, those monitoring the situation had a better sense of the situation's severity. But Smith still staunchly maintains that he didn't have full information on August 17. "I did not know the size, the scope of the breach," he told the committee. He finally notified the presiding director of Equifax's board on August 22, while the entire board of directors was briefed on August 24 and 25. "The picture was very fluid," Smith said. "We were learning new pieces of information each and every day. As soon as we thought we had information that was of value to the board I reached out."

Pretty leisurely timeline, no? There are still numerous outstanding questions, particularly about what Equifax general counsel John Kelly knew about the breach when he approved nearly $2 million in company stock sales for three executives at the beginning of August. But just these additional time stamps alone paint a picture of a severe lack of emergency protocol and general urgency.

2. Equifax's patching process was wholly inadequate. Attackers initially got into the affected customer-dispute portal through a vulnerability in the Apache Struts

Apache disclosed and patched the relevant vulnerability on March 6. In response to questions from representative Greg Walden of Oregon, Smith said there are two reasons the customer-dispute portal didn't receive that patch, known to be critical, in time to prevent the breach.

The first excuse Smith gave was "human error." He says there was a particular (unnamed) individual who knew that the portal needed to be patched but failed to notify the appropriate IT team. Second, Smith blamed a scanning system used to spot this sort of oversight that did not identify the customer-dispute portal as vulnerable. Smith said forensic investigators are still looking into why the scanner failed.

3. Equifax stored sensitive consumer information in plaintext rather than encrypt it. When asked by representative Adam Kinzinger of Illinois about what data Equifax encrypts in its systems, Smith admitted that the data compromised in the customer-dispute portal was stored in plaintext and would have been easily readable by attackers. "We use many techniques to protect data—encryption, tokenization, masking, encryption in motion, encrypting at rest," Smith said. "To be very specific, this data was not encrypted at rest."

It's unclear exactly what of the pilfered data resided in the portal versus other parts of Equifax's system, but it turns out that also didn't matter much, given Equifax's attitude toward encryption overall. "OK, so this wasn't [encrypted], but your core is?" Kinzinger asked. "Some, not all," Smith replied. "There are varying levels of security techniques that the team deploys in different environments around the business." Great, great.

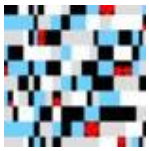
4. The recently resigned Equifax CEO only mandated security reviews every quarter. Toward the end of the hearing, Smith said he generally met with security and IT representatives once a quarter to review Equifax's security posture. Four meetings a year to defend hundreds of millions of people's crucial personal information gets you exactly the type of security posture Equifax had.

5. Equifax won't comment on, or rule out, nation-state attackers. There's no public evidence at all so far that a nation-state perpetrated the Equifax breach, but there have been some small hints that it could be a possibility. During Tuesday's hearing, Representative Walden mentioned in his opening statement that the breach has "markers of nation-state activity." But when pressed on the topic by representative Leonard Lance of New Jersey, former CEO Smith wouldn't answer. "I have no

is investigating the breach.

6. Equifax made its breach notification site a separate domain because its main site wasn't up to the task. One of the major blunders of Equifax's breach response was its decision to host an Equifaxsecurity2017.com notification site as a separate domain rather than on its established and trusted Equifax.com main site. Designing a totally distinct domain opened the Equifax breach response to a number of threats and vulnerabilities, including phishing sites masquerading as the satellite breach-response page. (In a moment of true dystopian chaos, the official Equifax Twitter account repeatedly tweeted a phishing link, mistaking it for the breach-response page.)

MORE EQUIFAX



LILY HAY NEWMAN
Equifax Officially Has No Excuse

LILY HAY NEWMAN
How to Protect Yourself From That Massive Equifax Breach

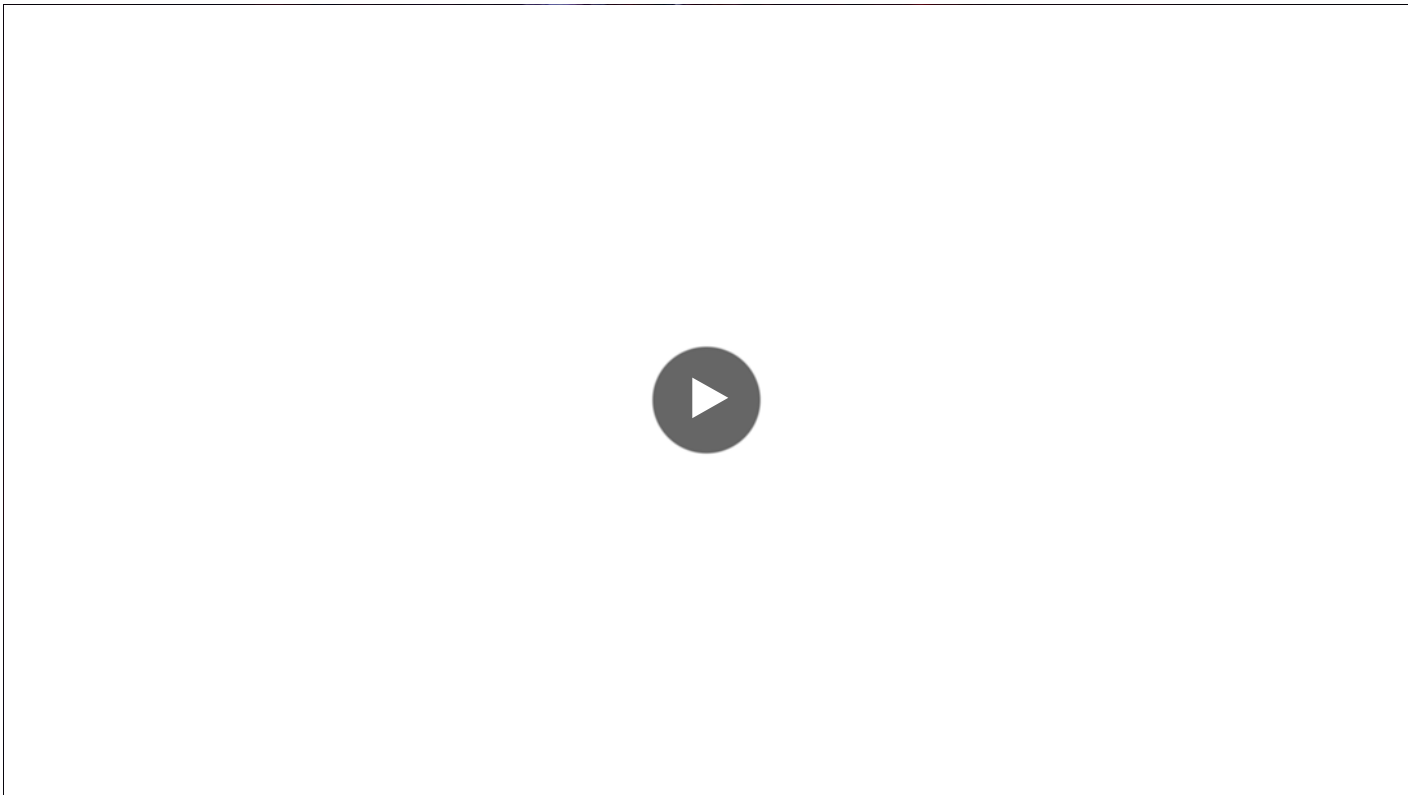
LILY HAY NEWMAN
The Equifax Breach Exposes America's Identity Crisis

When asked by multiple lawmakers why Equifax set up this separate site, Smith said the company's main domain was not architected to process the enormous traffic the company knew would come its way after the announcement. In all, Smith said, the independent breach-response site has had 400 million consumer visits, which would have crumpled the main site.

It's hard to even hold all the failures and missteps in your mind at once, but each revelation makes the overall picture seem that much uglier. "I just hope we get to the

"Because this is a mess."

RELATED VIDEO



SECURITY

Worried About Your Weak Passwords? Here's How to Fix Them

Look, we get it. Remembering dozens and dozens of different passwords for different sites is next to impossible. But that doesn't mean you should be reusing your passwords. That's just asking for trouble.

#EQUIFAX #DATA BREACHES #SECURITY #HACKS

VIEW COMMENTS

SPONSORED STORIES

MORE SECURITY

BREACHES

That Billion-Account Yahoo Breach Was Actually 3 Billion

LILY HAY NEWMAN

GUNS

Gun Control Tech Exists. But It Won't Stop Mass Shootings

LILY HAY NEWMAN

GUNS

How the Vegas Shooter Could've Gotten an Automatic Rifle

ANDY GREENBERG

[redacted]

Bad Info Follows Every Tragedy. Don't Fall For It

[redacted]

SECURITY

This "Ghost Gun" Machine Now Makes Untraceable Metal Handguns

ANDY GREENBERG

Inmates Need Social Media. Take It From a Former Prisoner

GET OUR NEWSLETTER

Enter your email

SUBMIT

RSS