



GDPR and What Else Is On Our Minds:

A Look at Data Protection and Cybersecurity in 2020

John Ansbach, JD/CIPP-US
Vice President, Aon Cyber Solutions
john.ansbach@aon.com

Overview

GDPR is important. We will talk about what it is and what it requires

But this isn't a GDPR session.

GDPR and other privacy and security regs are a response to what's been happening over the past several years with regard to enterprise data security – *the profound inability of for-profit and nonprofit enterprises to secure the data of their constituents*

In the time we have together, we're going to talk about what this landscape looks like as we start 2020, what trends we observed and expect to see into the new year, and what you should be focused on, not just to comply with GDPR and other applicable regulatory schemes, but how to best protect your data and ultimately, your nonprofit's mission.

Side Note

Whenever we discuss GDPR, people ask about CCPA and SHIELD. We won't get into these today, but so you know:

The **NY SHIELD Act** is the "Stop Hacks and Improve Electronic Data Security Act;" it went into effect on Oct 23, 2019

- Regardless of location or size, nonprofit orgs that receive, collect or otherwise possess private info about New York residents must comply with the New York SHIELD Act.
- Nonprofits with such data must adopt cybersecurity data safeguards that comply with the provisions of the SHIELD Act and are subject to notification requirements in the event of a data breach.

The **CA CCPA** is the "California Consumer Privacy Act;" it went into effect on Jan 1, 2020

- The statute defines covered businesses as those "organized or operated for the profit of its shareholders or other owners," so most nonprofits will not have to deal with CCPA
- That said, there is a school of thought out there that says that a nonprofit organization that controls or is controlled by a for-profit business covered under the CCPA will be subject to the CCPA.



Landscape



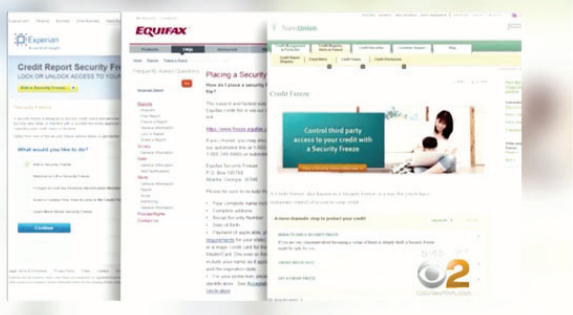
**EST. 500M
GUESTS AFFECTED
INFORMATION
AT RISK:**

- ADDRESSES
- DATES OF BIRTH
- PASSPORT NUMBERS

September 2017

Equifax CEO Retires Following Massive Data Breach

September 26, 2017 12:09 PM
Filed Under: Equifax



Equifax's top cybersecurity officers retire 'effective immediately'

By TARA SIEGEL BERNARD, TIFFANY HSU, NICOLE PERLROTH and RON LIEBER | SEPT. 7, 2017

SAN FRANCISCO — Equifax announced Friday afternoon its chief information officer, Susan Mauldin, and chief security officer, David Webb are retiring "effective immediately."

The departure of the two senior security professionals, charged with overseeing the credit reporting firm's defenses against hacks, follows the disclosure last week that hackers may have stolen personal data on 143 million of its U.S. customers, plus credit cards and personal identifying information for 400,000.

Webb is 61 and in 2016 received \$2.56 million in compensation, according to Reuters.

Mauldin was chief security officer at the company, one of the nation's three largest credit reporting firms, from 2013 until Friday. By Friday afternoon her name had disappeared from the company's website and her LinkedIn page only showed her first name and the initial of her last name, with her place of work listed as "private."

The breach happened because Equifax security staff failed to promptly install a security fix to a flaw found in a web application tool used by many major corporations, the industry group that oversees the open-source software said earlier this week.

Equifax had patch 2 months before hack and didn't install it, security group says

Hackers took advantage of a window when the flaw was known but not fixed, which lasted two months, to penetrate the company's digital defenses.

NEW YORK (CBSNewYork/AP) — Equifax CEO Richard Smith retired effective immediately on Tuesday, as the credit reporting agency tries to clean up the mess left by a damaging data breach that exposed highly sensitive information about 143 million Americans.

His departure follows those of two other high-ranking executives after Equifax disclosure that hackers exploited a software flaw that the company didn't fix to access people's Social Security numbers, birthdates and other personal data that provide the keys to identify theft.

STROZ

AON
Empower Results®

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](https://utcle.org/elibrary)

Title search: GDPR and What Else Is On Our Minds: A Look at Data Protection and Cybersecurity in 2020

Also available as part of the eCourse
[2020 Nonprofit Organizations eConference](#)

First appeared as part of the conference materials for the
37th Annual Nonprofit Organizations Institute session
"GDPR and What Else Is On Our Minds: A Look at Data Protection and Cybersecurity in
2020"