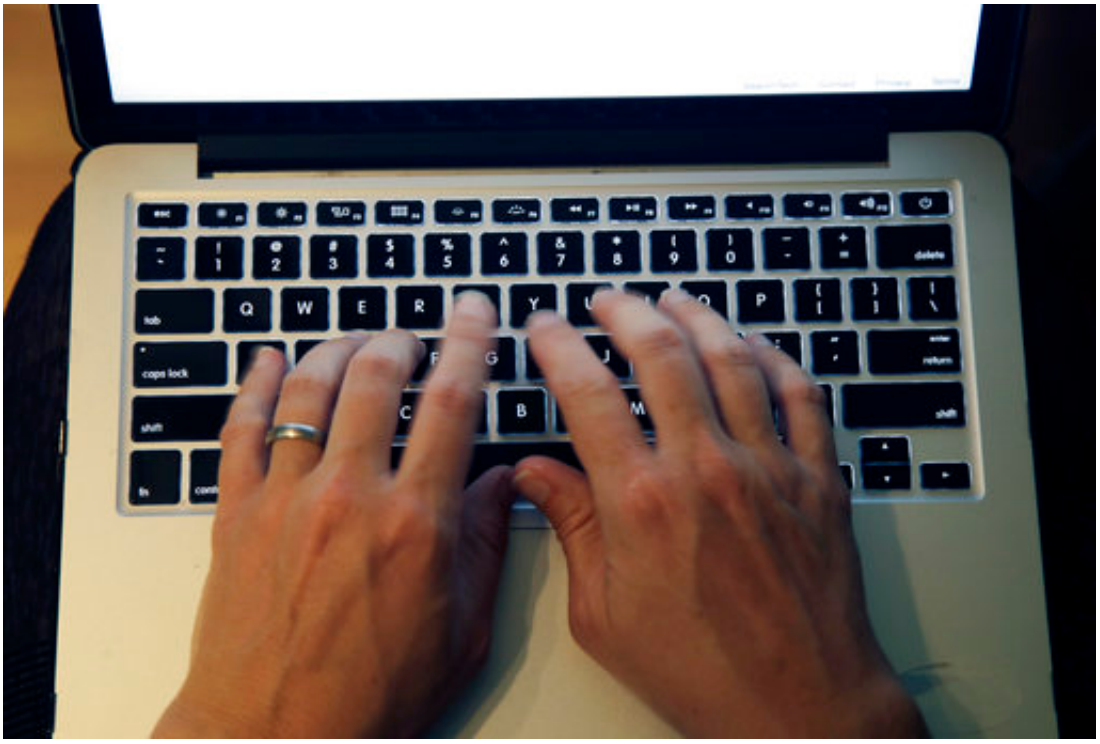
# How to fix identity-theft issues posed by the Equifax hack

September 11 2017, by Matt O'brien And Anick Jesdanun



This Monday, June 19, 2017, photo shows fingers on laptop keyboard in North Andover, Mass. The Equifax breach not only exposed sensitive personal information of 143 million Americans, but it also underscored the huge and largely unaddressed vulnerabilities that make widespread identity theft possible. Experts have warned for years that the widespread use of Social Security numbers, lax corporate security and even looser individual password practices could lead to an identity-theft apocalypse. (AP Photo/Elise Amendola)

The Equifax breach didn't just expose sensitive personal information of 143 million Americans—it underscored the huge vulnerabilities that make widespread identity theft possible.

More than 15 million Americans were victims of ID fraud last year, a record high; fraudsters stole about $16 billion, according to an annual survey by Javelin Strategy & Research. The theft of personal information can turn peoples' lives inside out, damage their finances, eat away at their time and cause tremendous anxiety and emotional distress.

The Equifax attack was particularly damaging. Intruders made off with precisely the information needed to pose as ordinary citizens and defraud them—and did so with data for roughly 44 percent of the U.S. population.

Experts have warned for years that the widespread use of Social Security numbers, lax corporate security and even looser individual password practices could lead to an identity-theft apocalypse.

As Congress, state law enforcement and the nation's chief financial watchdog look into the Equifax debacle, here are some of today's biggest security problems and what it could take to fix them.

___

SOCIAL SECURITY NUMBERS

A decade ago, computer scientist Annie Anton warned Congress that widespread business use of Social Security numbers as identifiers was making them more attractive to identity thieves. "This is a problem of our own making and it is a problem that we can eliminate," she testified to a House committee in June 2007.

Yet the problem remains un-eliminated. Anton, now a Georgia Tech researcher whose office isn't far from Equifax's Atlanta headquarters, argues that SSNs should be encrypted to shield them from prying eyes, much like passwords are. Equifax apparently didn't take this precaution , a fact Anton calls "shocking." The company didn't immediately respond to requests on Monday for more information about its encryption practices.

Some advocates would like to outlaw the use of Social Security numbers by private companies, and even by government agencies outside of the Social Security Administration. Such efforts have gone nowhere, although several states have passed a patchwork of laws aiming to limit access to SSNs and other sensitive information.

Further changes may simply be too late. Even before the Equifax breach, millions of SSNs were already exposed from various hacks—and no one can change them without enormous hassle.

One alternative might be to replace the venerable SSN with a national ID card protected with encryption, much the way credit cards with embedded chips work today. Knowing the number alone wouldn't be enough; a thief would need the physical card as well. But while other nations have adopted such cards, many Americans have traditionally resisted a national ID.

As Ryan Kalember, senior vice president of cybersecurity strategy at the security company Proofpoint, says, it's time to address "why we rely on these trivial and compromised pieces of information for some of the most important financial transactions we make."

___

LAX CORPORATE SECURITY

Security is ultimately an expense on a company's financial sheets, an important function that produces neither revenue nor obvious benefits (though any failures are immediately obvious).

As a result, many security departments are underfunded or lack the authority to impose sound security practices across the company—including on employees who write software, said Rich Mogull, who runs the security research firm Securosis. And those other employees sometimes make mistakes that lead to breaches, Mogull said.

"Those most responsible ... don't have the economic incentives to actually make it a priority," Mogull said.

It might also help if more top executives lost their jobs after a major breach, Mogull said. A massive data breach at Target in 2014, for instance, contributed to the departure of CEO Gregg Steinhafel.

"Boards are now feeling the pressure and responsibility to make sure this stuff doesn't happen," said David Hickton, a former U.S. attorney who now directs a cyberlaw institute at the University of Pittsburgh.

But even at companies that give security top priority, the risk is never zero. "Companies can build the proverbial 10-foot firewall around their network and sensitive information, but criminals are always going to find that 11-foot ladder," said Craig Newman, a privacy and data-security attorney at the Patterson Belknap Webb & Tyler law firm.

___

BAD, BAD PASSWORDS

Though Equifax blamed an unspecified "website application vulnerability" in its attack, a more common risk is bad passwords,

Kalember said. A breach in one easy-to-guess employee password can get hackers in the door. Once inside, other systems on the network are typically unprotected.

But getting people to adopt strong passwords is difficult—who can remember seemingly random strings of characters for dozens or hundreds of services? Password managers can securely store strong, randomized passwords, but most people don't use them. The fallback for many people is to reuse passwords, which means that when one service gets hacked, other accounts are also vulnerable.

Ultimately, passwords should be just one of many ways to authenticate one's identity, Kalember said.

Two-factor authentication—which asks users to enter a second form of identification, such as a code texted to their phone—can provide additional protections. But it's not always available, and it can be cumbersome for those who aren't tech-savvy.