The SSN - Why Are We Still Using a 1930s Identifier as a 21st-Century Security Credential?

March 17, 2026 - A newly discovered online database containing roughly 184 million login credentials is the latest reminder that Americansâ€™ personal information continues to circulate widely on the internet. Security researchers say the exposed data included email addresses, passwords, and login information connected to a variety of online accounts. But the real story is not the latest data leak. In fact, we're at the point that that "who" and "how" of it don't really matter anymore. The real issue is that the system Americans rely on to prove their identity was never designed to survive the digital age, and unless changes are made these breaches will continue to happen with predictable reliability.
For years, lawmakers have responded to data breaches with new rules requiring companies to report them, notify customers, and sometimes pay fines. Those steps may help consumers learn their information was exposed. They do very little to stop identity theft in the first place.

The uncomfortable truth is that the technology already exists to make most stolen data far less useful to criminals. The problem is that the U.S. identity system still relies on permanent identifiers - especially the Social Security number - that function like passwords that never change. Once a criminal has that number, they often have it forever.

That design flaw explains why a breach at one company can cause problems years later. The same Social Security number can be used again and again across banks, credit applications, medical records, and tax filings. But there are several relatively simple changes that could dramatically reduce identity theft without building an entirely new government system, which would inevitably become a target for hackers.

One approach is already familiar to many credit card users. Some banks now allow customers to generate temporary credit card numbers for online purchases. The number works for a single merchant or a single transaction and then expires. If hackers steal it, the information is essentially useless.

The same concept could be applied to identity information.

Instead of giving a company a permanent Social Security number, a system could provide a temporary identification code that only works for that specific transaction. If a company is hacked, the stolen number could not be used elsewhere.

Another change could involve how credit reports are handled. Today, criminals often open credit cards or loans in someone elseâ€™s name using stolen personal data. Consumers can protect themselves by freezing their credit files, but many people do not know about the option or forget to do it. An analysis by LendingTree found that only 9.9% of Americans have frozen their credit files, meaning the vast majority of credit reports remain open to potential misuse. But if credit files were frozen by default and consumers simply approved requests when they apply for credit, that single step would prevent many fraudulent accounts from ever being opened.

Neither of these ideas require futuristic technology. The payment industry already uses similar tools to protect credit card transactions every day. Yet public policy debates about data security often focus on what companies must do after a breach occurs rather than redesigning the system that makes stolen information valuable.

That may reflect another problem: many policymakers simply have not spent the time to understand how identity theft actually works in a digital economy. The result is a system where Americans are repeatedly told their information may have been exposed, while the underlying architecture that enables identity theft remains largely unchanged.

And the foundation of that architecture dates back nearly a century. The Social Security number was created in 1936 to track workersâ€™ contributions to retirement benefits. It was never designed to serve as a universal identity credential. Over time, however, businesses and government agencies began using it because it was convenient. Banks adopted it to match financial records. Credit reporting companies used it to organize credit histories. Employers used it for payroll reporting. Eventually, the number became the easiest way for institutions to identify individuals across multiple systems.

The U.S. never formally chose the Social Security number as a national ID system. It simply evolved into one because it was convenient for bureaucracies and businesses alike.

What began in 1936 as a bookkeeping number became the backbone of identity verification across the economy. It is now time to restructure it. Not doing so just ensures that the next data breach is right around the corner and that it will be used by criminals for more fraud.
by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS