CLERESTORY ADVISORS

Enlightened Financial Planning

The Total Breach

Is your personal data at risk? The answer is always yes, but it may be more widely available now than it was a year ago.

According to recent court filings, the Department of Government Efficiency (DOGE) was a bit careless with the Social Security files that the Administration maintains of Americans, including those who have claimed for Medicare or Social Security benefits. The database holds names, dates of birth (and place), gender, address, citizenship status, income, employment history, the names of both parents, Social Security numbers and private log-in credentials. Much of this information is also compiled and stored on every person who has obtained a Social Security number, meaning that it's not just older people whose data would be compromised.

Compromised how? In a court filing on January 16 of this year, members of the Trump Administration's Justice Department's legal team wrote to the judge that DOGE employees were sharing their downloaded SSA data to DOGE staffers working outside the agency through an unapproved third-party server. The government attorneys also acknowledged that one DOGE staffer sent downloaded data to a political advocacy group after it asked for the information so it could analyze voter rolls "to find evidence of voter fraud and to overturn election results in certain states." Where that data went after that has not been determined.

There may have been other data leaks. On March 25, President Trump announced an executive order directing the Social Security Administration to take all appropriate action to make SSA databases accessible to election officials verifying voter registrations.

This trove of information is of nearly infinite value to the criminal underworld. If a number of people had access to it, there would be an enormous temptation to quietly sell the SSA database to the highest bidder—and there may have been a number of such sales, enriching the net worth of a few young DOGE staffers who might have been unhappy when the DOGE initiative unraveled and they were dismissed from service.

The news is full of major breaches at banks, credit card companies and retailers, all of which allow private information to flow into the dark web, where it can be weaponized by scammers and the sort of people who apply for loans and credit cards in the names of other people. This breach is potentially larger than all of those combined, and it suggests that you, me and all of us should take extra precautions like:

- Freezing our credit at the credit bureaus- https://www.usa.gov/credit-freeze).
- Making our passwords more complex and considering using a password manager.

- Monitoring our bank statements for unauthorized transactions—including anything suspicious that might have happened since last February or March.

And if someone calls and seems to know everything about you, make sure you actually know that person—because it's possible that anyone trolling the dark web is now familiar with your personal details.

Sources:

https://www.npr.org/2026/01/23/nx-s1-5684185/doge-data-social-security-privacy

https://www.ssa.gov/policy/docs/ssb/v65n2/v65n2p95.html

https://www.hks.harvard.edu/faculty-research/policy-topics/science-technology-data/doge-putting-countrys-data-and-computing

By Bob Veres, publisher of Inside Information - the premier publication of financial industry trends and information for leading practitioners in the financial planning profession.