EXHIBIT B

EXCLUSIVE

Whistleblower claims ex-DOGE member says he took Social Security data to new job

The Social Security inspector general's office is investigating allegations that the former DOGE engineer took sensitive data on a thumb drive in a major potential security breach, said people familiar with the process.

March 10, 2026

By Meryl Kornfield, Elizabeth Dwoskin and Lisa Rein

Meryl Kornfield and Elizabeth Dwoskin can be reached securely on Signal at @merylkornfield.59 and @lizza_dwoskin.42

The Social Security Administration's internal watchdog is investigating a complaint that alleges a former U.S. DOGE Service employee claimed he had access to two highly sensitive agency databases and planned to share the information with his private employer — a claim that, if true, would constitute an unprecedented breach of security protocols at an agency that serves more than 70 million Americans.

The agency's inspector general is investigating the disclosure and has alerted members of Congress of its existence, according to a letter by the acting inspector general to top members of four congressional committees reviewed by The Washington Post and two people familiar with the process, who spoke on the condition of anonymity to describe sensitive deliberations. The inspector general's office has also shared the disclosure with the Government Accountability Office, which has been conducting its own audit of DOGE's access to data, according to one of the people. The Post has reviewed the complaint and spoken with the whistleblower, who issued the complaint anonymously for fear of retaliation.

According to the disclosure, the former DOGE software engineer, who worked at the Social Security Administration last year before starting a job at a government contractor in October, allegedly told several co-workers that he possessed two tightly restricted databases of U.S. citizens' information, and had at least one on a thumb drive. The databases, called "Numident" and the "Master Death File," include records for more than 500 million living and dead Americans, including Social Security numbers, places and dates of birth, citizenship, race and ethnicity, and parents' names. The complaint does not include specific dates of when he is said to have told colleagues this information, but at least one of the alleged events unfolded around early January, according to the complaint. While working at DOGE, the engineer had approved access to Social Security data.

According to the complaint, he allegedly told the whistleblower that he needed help transferring data from a thumb drive "to his personal computer so that he could 'sanitize' the data before using it at [the company.]" The engineer told colleagues that once he had removed personal details from the data, he wanted to upload it into the company's systems. He told another colleague, who refused to help him upload the data because of legal concerns, that he expected to receive a presidential pardon if his actions were deemed to be illegal, according to the complaint.

The complaint does not allege that the engineer was successful in uploading the data to the company's system.

The Post is not naming the former DOGE member or company because it has not independently confirmed the accusations in the complaint.

The whistleblower filed the complaint with the inspector general in January. When The Post contacted the agency and the company in January, both said they had not heard of the complaint. Both said they

subsequently looked into the engineer's actions and not find evidence to corroborate the claims. The company said it had conducted a "thorough" two-day internal investigation and concluded the assertions were unsubstantiated. Reached this week, both declined further comment.

A lawyer who represents the former DOGE member told The Post he denied all alleged wrongdoing.

The complaint alleges that after leaving government employment, the former DOGE member told colleagues he had a thumb drive with Social Security data and had kept his agency computer and credentials, which he allegedly said carried largely unrestricted "God-level" security access to the agency's systems — a level of access no other company employee had been granted in its work with SSA.

The agency has historically limited access to sensitive data to prevent it from leaking. But the Supreme Court had granted DOGE members "unfettered" access to Social Security data last summer, though that did not apply to outside contractors.

An SSA official familiar with the former DOGE member's current status said the engineer had lost his data credential privileges and turned in his SSA laptop when he departed the agency.

The whistleblower disclosure — filed with the agency's inspector general office on Jan. 9 and amended on Jan. 26 — alleges that the former DOGE member told the whistleblower that he was permitted to have unfettered access to Americans' Social Security data.

Democrats who were informed by the Government Accountability Office and the inspector general's office about the existence of the complaint raised concerns that the allegations could confirm their fears that DOGE acted without regard for data privacy.

"Not only has an ex-DOGE bro been accused of running around with the Social Security information of every American on a flash drive, he also may have the ability to edit and manipulate data at the Social Security Administration at will," Rep. Robert Garcia (California), the top Democrat on the House Committee on Oversight and Government Reform, said in a statement. "This is dangerous and outrageous, and Oversight Committee Democrats will fight for transparency and accountability."

The allegations stoke concerns about whether sensitive agency data on U.S. citizens may have been inappropriately accessed and shared during the tumultuous period when DOGE gained power within the government early last year. At the time, President Donald Trump empowered billionaire businessman Elon Musk to run a signature White House cost-cutting initiative that would drill into agency information to search for waste, fraud and programs that went against the administration's priorities.

SSA spokesman Barton Mackey said in a statement before the IG launched its investigation that "the allegation by a singular anonymous source has been found to be false based on evidence and investigations by all involved."

When asked about the whistleblower complaint, Leland Dudek, former acting commissioner of the agency during the beginning of DOGE's work, said he was unaware of the details of the allegations but said such actions would not comply with the rules at the agency regarding government data sharing.

"Sharing Numident data with unauthorized third parties, whether via the cloud or a personal thumb drive, violates the law," Dudek said.

A separate complaint, made in August by the agency's former chief data officer, Charles Borges, alleges members of DOGE improperly uploaded copies of Americans' Social Security data to a digital cloud, putting individuals' private information at risk. In January, the Trump administration acknowledged DOGE staffers were responsible for separate data breaches at the agency, including sharing data through an unapproved third-party service and that one of the DOGE staffers signed an agreement to share data with an unnamed political group aiming to overturn election results in several states.

When Musk created the DOGE cost-cutting project last year, he made swift changes to government agencies by accessing their tech systems, according to four people familiar with his strategy, three of whom spoke on the condition of anonymity to describe private conversations. Soon, DOGE engineers were deployed across the federal government, retrieving heavily restricted government databases and merging long-siloed repositories to hunt down possible evidence of fraud or diversity initiatives.

A dozen DOGE workers were embedded at Social Security headquarters starting in February 2025, after the Trump administration installed Dudek as acting commissioner. Most of the team were tech experts and engineers. Team members never appeared on SSA's organizational chart, leading to

experts and engineers. Team members never appeared on SSA's organizational chart, leading to confusion about their presence and roles within an agency known for safeguarding Americans' financial data, said one of the people, who had direct knowledge of DOGE's activities within the agency.

Their team was tasked with finding fraud in the Social Security rolls, especially seeking evidence of benefits going to dead people, the person said. Social Security technologists frequently pushed back against these presumptions of widespread fraud, but DOGE staff continued in their quest.

The "DOGE boys had … pre-ordained answers and weren't interested in anything other than defending decisions they'd already made," the person said.

Borges told Congress and reporters in August that DOGE members had access to data that had been blocked by a judge's order and that the DOGE team used unsanctioned methods to put data into the cloud.

Borges's attorneys said in the complaint that DOGE members received uninhibited access to sensitive data and potentially violated internal security protocols and federal privacy laws.

Borges's disclosure cited a June 2025 email thread in which SSA officials discussed allowing the DOGE member to copy and access one of the sensitive databases, Numident. One of the officials requested a sign-off by the agency's DOGE-aligned top IT official before they would hand over any data because it was an unusual request. The IT official granted the request, according to Borges's disclosure.

Social Security initially denied Borges's allegations and said the data referenced in his complaint is stored in a secure environment walled-off from the internet.

But in January, the Justice Department acknowledged in court documents that DOGE members had accessed and shared sensitive Social Security data without the awareness of agency officials.

Borges's attorneys were told this year that the Office of Special Counsel would stop reviewing his allegations while the GAO conducts a government-wide review of DOGE's access to sensitive data. However, the GAO audit does not provide protections to whistleblowers, raising concerns from legal experts that it will be difficult for people with sensitive information to come forward.

Jessica Baxter, a GAO spokeswoman, confirmed in an email to The Post that GAO's review is ongoing and she did not provide a timeline for when a report would be issued.

Borges said he feared that the government will never be able to determine what happened to the data after it was no longer in the sole possession of the agency.

"This is absolutely the worst-case scenario," Borges told The Post. "There could be one or a million copies of it, and we will never know now."

Aaron Schaffer contributed to this report.