DOGE

Court Documents Shed New Light on DOGE Access and Activity at Treasury Department

New court documents shed light on what a 25-year-old DOGE worker named Marko Elez did inside Treasury Department payment systems, including what Treasury staff did to limit his access. The documents indicate that the situation is more nuanced than previously reported.

Kim Zetter
Feb 13, 2025 • 15 min read

U.S. Department of Treasury building in Washington, DC. Photo: Carol M. Highsmith Archive, Library of Congress

Contrary to previous government statements, Marko Elez, a controversial 25-year-old employee working temporarily at the Treasury Department for Elon Musk's

Department of Government Efficiency (DOGE), *did* have "write" privileges to one sensitive Treasury Department payments database in February. His access was the equivalent of data-editing privileges, however, not administrative-level network access as previously reported, and the "write" privilege was given to him by mistake for one day before Treasury discovered the error and revoked the privilege, according to an affidavit filed this week by a Treasury executive. There is no sign that Elez altered anything in the database before Treasury staff changed his access privileges.

The information contradicts not only previous government statements that Elez had only "read-only" access to Treasury payments systems, it also contradicts previous news stories reporting that Elez had administrative-level network privileges that would have allowed him to alter anything on Treasury's network – from bypassing security measures to changing access privileges for users and altering source code on production systems.

According to signed affidavits filed on Tuesday by Treasury Department career executives defending the access they provided Elez, their staff implemented a number of security restrictions around Elez's access to Treasury systems. He was the only DOGE worker given direct access to the systems, for example, and he was prohibited from using his own laptop to access them. Additionally, he could only connect using a government-issued laptop that had "cybersecurity tools" installed on it to prevent him from accessing web sites or cloud-based storage services with the laptop or connecting a USB or other external storage device to it to copy large amounts of data from Treasury systems.

The information contradicts previous news stories reporting that Elez had administrative-level access that would have allowed him

to alter anything on the network, including bypass security measures, change access privileges for users or alter source code on production systems.

The information appears in an affidavit filed Tuesday by Joseph Gioeli III, a career technology executive who oversees information and security services at the Treasury Department's Bureau of the Fiscal Service (hereafter referred to as BFS or the Bureau). The Bureau, a nonpartisan entity, oversees Treasury systems and networks that process and disburse payments on behalf of nearly 250 federal agencies, including Social Security benefits and foreign aid.

Affidavit of Joseph Gioeli

Affidavit of Joseph Gioeli.pdf • 117 KB

Gioeli told the court that his staff established a number of security measures at the start of Elez's employment in January to restrict and monitor his access to Treasury payment systems and prevent unauthorized activity, such as exfiltrating data or sharing it with unauthorized parties. Gioeli acknowledges, however, that Elez may have "occasionally" taken screen shots of payment system data or records to share with a second DOGE employee working with him at Treasury.

Elez worked for the government just a few weeks before resigning on February 6 after the *Wall Street Journal* discovered a series of racist posts he allegedly posted to social media accounts before he joined DOGE in January. Although President Donald Trump and Vice President JD Vance have since called for Musk to re-hire Elez, the youth has so far not been re-instated in his job.

Gioeli submitted his affidavit on February 11 as part of a lawsuit filed against President Trump and the Treasury Department by 19 mostly Democratic attorneys general from around the country seeking an emergency temporary restraining order to limit access by DOGE employees to Treasury payment systems. The plaintiffs have argued that DOGE workers have no legal authority to access the highly sensitive Treasury systems and could cause disruption to critical payments or undermine the security of the systems.

Lawsuit for Temp Restraining Order Against DOGE Access at Treasury

Lawsuit for Temp Restraining Order Against DOGE Access at Treasury.pdf • 647 KB

The suit was filed in New York on February 7 after two news stories reported that Elez had the ability to make high-level changes to Treasury systems. Wired Magazine reported on February 4 that Elez had been given read-write privileges on "two of the most sensitive systems" at the Treasury Department, giving him the ability to change code on the systems. Wired also wrote that Elez had "many administrator-level privileges" that would typically give someone the ability to navigate through parts of the system that ordinary users can't access, delete or add system files to alter how the system operates, change user permissions to give others access to the system, and delete or modify critical files to allow him or others to bypass security measures.

Wired didn't say whether Elez had made any changes, but the same day, Josh Marshall of Talking Points Memo, reported that Elez did make changes to source code underlying the operation of the payment systems. Marshall wrote that Elez made the changes directly to a production system, without first testing them in a development environment to ensure they would not disrupt the system, and that the

changes were designed to create "new paths to block payments and possibly leave less visibility into what has been blocked."

The allegations raised alarming questions about whether DOGE workers were halting Treasury payments with abandon or altering highly sensitive payment systems in ways that could disrupt their operation or undermine their security. On Saturday U.S. District Judge Paul Engelmayer in New York granted the restraining order to temporarily block DOGE's access to Treasury's payment systems until more information could be obtained about what workers were doing there.

Gioeli's affidavit, filed after the judge's order, disputes the reported claims and explains how Treasury staff say they carefully handled DOGE access to the payment systems to ensure the security and integrity of the systems. The affidavit suggests that media outlets, or their sources, may have conflated different things and misunderstood what was occurring at Treasury.

> If you know anything about what is going on inside government agencies with regard to DOGE, or anything else, please contact me on Signal at KimZ.42.

Background

On January 20 this year, President Trump signed an executive order creating DOGE as a temporary department in the Executive Office of the President. It also directed leaders at federal agencies to establish a DOGE team at each agency —consisting of at least four people – to work on modernizing federal systems and software to make them more efficient. The same day, Trump signed a second executive order – entitled “Reevaluating and Realigning United States Foreign Aid” – which ordered a 90-day pause on all federal government payments issued for foreign development assistance. Since many of these payments get issued through Treasury Department payment systems, the DOGE team assigned to Treasury was one of the first to get set up.

Thomas Krause, Jr., former CFO and President of Broadcom Software and current CEO of the Cloud Service Group, was put in charge of the DOGE team at Treasury. Specifically, he was made senior advisor for technology and modernization at Treasury in January – a temporary and unpaid special government employee position. Elez was hired to serve as Krause's technical lead and advisor and was the only one of the two who was given direct access to Treasury systems. Krause only had "observation access," according to Gioeli, meaning he had the ability to look over the shoulder of Elez or others as they accessed Treasury payment systems or source code but couldn't access the systems himself.

Elez, who began working as a Treasury employee on January 21, was supposed to work with engineers at the Bureau to find ways to update and modernize payment systems to improve their efficiency and make it easier to track payments and identify potentially improper and fraudulent ones. Treasury staff developed a 4-6 week "engagement" plan to provide DOGE workers with access to and information about several payment systems. These Treasury systems included:

Payment Automation Manager (PAM) - an application for processing payments disbursed by federal agencies. Sometimes called the "landing zone" this is where federal agencies send a payment file (essentially a request to make a payment). When an agency submits a payment file, the system validates the file and sends a report back to the federal agency, indicating if the payment is potentially improper or fraudulent. If it's a valid payment, the federal agency then certifies the payment in the SPS system (below), after which the payment gets processed and disbursed.

Secure Payment System (SPS) - another payment-processing system through which federal agencies create, certify, and submit payment files, including for one-time large dollar amount transactions.

Automated Standard Application for Payments (ASAP) - a system that allows recipients of a payment to draw funds from an account set up for them.

International Treasury Services (ITS) - system through which federal agencies can make international payments; it's often used to distribute Social Security benefits to Americans living abroad.

Central Accounting and Reporting System (CARS) - an accounting system for recording the financial data related to an agency’s spending.

DOGE Access Restrictions

Elez was supposed to get access to source code, applications, and databases across all of these systems. But such access comes with many risks. It can potentially lead to disruption in the payment systems if a user doesn't know what they're doing and makes a mistake, the user can improperly access or use sensitive data, and the user can introduce unintentional vulnerabilities to the system or conduct malicious activity inside it.

To address these risks, Gioeli says his Treasury staff implemented several safeguards:

Elez could not use his own computer to access Treasury systems or even a general laptop the Treasury Department had given him. Per Bureau security policies, he had to be given a Bureau-specific laptop to access the source-code repository and payment systems. The laptop was encrypted to prevent unauthorized access to it if lost or stolen.

BFS used "several cybersecurity tools" to continuously monitor and log Elez’s activity – tools that blocked his access to web sites, blocked the use of external peripherals (such as USB or external storage drives), monitored any scripts or commands he tried to execute on the device, and blocked access to cloud-based storage services. His laptop also had data-exfiltration detection to alert the Bureau if he tried to transmit any sensitive data.

On January 28, the Bureau gave Elez his Bureau laptop as well as access to copies of source code for the PAM, SPS, and ASAP systems, which he could only examine inside a “secure code repository” or sandbox environment. Elez could make changes to the source code copies in the sandbox, but Gioeli insists he did not have the authority or ability to publish any code changes to the production system, as Talking Points Memo had reported, or even to any test environment. Elez could only "review and make changes locally to copies of the source code" in the cordoned-off code repository. "This repository was separate from Fiscal Service’s typical code development environment, and unlike the usual code development environment, this new repository was segmented, to ensure that no changes to the operative source code could be made," Gioeli wrote in his affidavit.

According to Gioeli, beginning on February 3, Elez was given access to at least two Treasury payment systems – the PAM database and file system. He was given read-only privileges on them, which meant he could only view and query the information on the systems, not make changes to the data. He also received a “walk-through” demonstration of the PAM database and file system to learn how they worked. Gioeli says Elez's access to these systems was closely monitored by multiple administrators in addition to being tracked by security tools.

On February 5, Elez received access to Treasury's Secure Payment System (SPS) database – the system federal agencies use to create, certify, and submit payment orders to Treasury. Staff gave him a virtual over-the-shoulder walk-through to help him connect to the database, and Gioeli says he accessed it "exclusively under the supervision of Bureau database administrators," and didn't access it again after this.

According to Gioeli, his access to the SPS database should have been read-only, but the next morning staff discovered that he had mistakenly been given read-write permissions, giving him the ability to alter data on the system. Administrators immediately changed his privileges to "read-only" then began a forensic review of all

activity that had occurred on the server, the database and Elez's laptop. They found that Elez had only accessed the SPS once on February 5th when Treasury employees gave him their guided tour through the system, and he did not log in again after this or engage in any unauthorized activity while he had been on it.

Gioeli says he doesn't believe Elez even knew he had "write" privileges when he was on the system and in any case "never took any action" to exercise those privileges to modify anything. He notes, however, that forensic analysis is still ongoing to confirm this.

Gioeli says the staff never got around to giving Elez access to the ASAP, CARS, or ITS systems before he resigned on February 6. After he submitted his resignation, he turned in his Treasury laptop, his Bureau laptop, building access cards and government cell phone, and staff terminated his access to Bureau systems. It's unclear if Treasury system administrators discovered they had mistakenly given Elez "write" privileges to the SPS database before he resigned that day or only afterward when they moved to disable his access to the network.

Jake Williams, vice president of research and development at the cybersecurity consultancy Hunter Strategy, says the steps the Treasury staff took to ensure Elez didn't exceed the level of authorization he was granted sound "reasonable."

"It’s a baseline set of controls," he says. "I think they took the steps they should have taken." But he notes that the thoroughness of any forensic investigation they conduct into what Elez may or may not have done on his laptop or on the network depends on the thoroughness of their logging capabilities. Without knowing how much logging they were doing, it's hard to say whether their investigation is thorough.

"In a lot of cases, we simply don’t have the data available to say for instance a particular action was taken by a particular person. It all relies on application-level logging, which in some cases doesn’t exist."

Although the unauthorized write access was discovered on February 6, Gioeli says the review of Elez's laptop logs is still ongoing to determine everything he did on the device. Based on preliminary log reviews his activity included the following:

On February 3, Elez copied two US AID files from the PAM database to his Bureau laptop (US AID refers to the United States Agency for International Development); on February 4 and 5, he accessed the PAM file system; and on February 5, he accessed the PAM payment processing database.

"These activities are consistent with the read-only access that Mr. Elez was provided and [he] did not change or alter any Bureau payment system or record within their source systems," Gioeli noted in his affidavit.

Was the Reporting Wrong?

All of this raises questions about previous reporting on what happened at Treasury. Did Wired, or its sources, get the story wrong in reporting that Elez had administrative-level privileges on Treasury payment systems?

It's possible that the reporters or their sources conflated "write" privileges to a database with administrative privileges on a network. Administrative privileges aren't generally referred to as "write" privileges. Possessing writing privileges for a database means that someone can add, delete or alter data in the database, but this has nothing to do with the ability to change underlying source code for the database or make the kind of network configuration changes that Wired described in its story.

It's notable, however, that Wired reported on February 4th that Elez had "write" privileges to Treasury payment systems. According to Gioeli he only obtained "write" privileges to one database on February 5th, the day *after* the Wired story published. This raises questions about whether Treasury had intended to give him "write" access to the database all along, prompting an inside source to disclose this to

Wired the day before administrators actually gave him that access, or whether Wired's sources confused the ability to alter a copy of source code with "write privileges" and administrative-level network access.

It's worth asking, however: would Treasury Department administrators have even discovered that they had mistakenly given Elez unauthorized "write" permission to the SPS system if Wired hadn't published its story? Did the story cause administrators to scrutinize Elez's access more closely and uncover their mistake? It's hard to say. The story and subsequent lawsuit have, however, put Treasury staff on notice that they have to be very intentional and cautious about everything they allow DOGE workers to do on Treasury systems going forward.

Did Elez Make Changes to Treasury Source Code?

In Josh Marshall's Talking Points Memo article, he reported that sources told him Elez had made changes to the payment system source code to create "new paths to block payments and possibly leave less visibility into what has been blocked."

Gioeli doesn't indicate if Elez actually made any code changes, only that he did not have the ability to make changes directly to code on production systems. He could only make changes to a copy of the source code stored in a sandbox environment. But there is one other court document that does reference a change Elez made, in conjunction with Bureau staff. According to a separate affidavit filed by another career civil servant at Treasury named Vona Robinson, deputy assistant commissioner for federal disbursement services at the Bureau, Elez may have made a change to help staff more quickly identify specific types of payments in the system.

Affidavit of Vona Robinson

Affidavit of Vona Robinson.pdf • 118 KB

Under the President’s January 20 Executive Order temporarily halting foreign development payments for 90 days, it gives Secretary of State Marco Rubio the ability to issue waivers to allow some payments to go through.

To make such determinations, the Bureau was supposed to make a copy of any request for foreign aid payments – especially requests coming from US AID – and send the copies to a secure portal for the secretary of state's office to review. Initially, Treasury department staff were manually querying the database to identify payment requests that might require review by the secretary of state. But according to Robinson at some point after January 31, Elez "assisted in automating the manual review of the payment files." This suggests that he, along with Bureau IT staff, may have made a change to the system's code to accomplish this.

A source told Talking Points Memo that the code changes Elez made created "new paths to block payments." But this may actually refer to the change Elez and Bureau staff made to send a copy of foreign aid payment requests – which were supposed to be temporarily blocked per the president's executive order – to a secure portal for the secretary of state to review.

Notably, Robinson says that only two sets of payments got copied and flagged for the secretary of state to review during this time period. The first occurred on February 7 and involved three payment requests made by the Department of Health and Human Services. The secretary of state determined that these payments did not fall under the Executive Order's mandatory payment halt and allowed the payments to be processed. The second set was flagged on February 10. It was an international payment submitted by the Millennium Challenge Corporation, a congressionally created entity that provides investment to poor countries that are committed to democratic governance and economic freedom. According to Robinson, the MCC withdrew its payment request the same day it submitted it.

In any case, after Elez helped devise a method to make copies of foreign aid payment requests and send them securely to the secretary of state's office for review, the latter figured out a way to get copies of the payment requests prior to them entering the Treasury system, according to the court documents. So the solution Elez helped devise wasn't needed.

Robinson writes that "To the best of my knowledge, BFS has not failed to disburse any payment duly certified by a payor agency as a result of the Treasury DOGE Team's work. To date, no payments, with the exception of the single MCC payment mentioned above, have been delayed or canceled by the payor agency as a result of the re-routing and review process described herein."

Update Feb 14: On Friday, the Treasury Department's Office of Inspector General announced it would launch an audit of DOGE's access into Treasury Department systems as well as security controls around its payment systems. It will also include a review of the past two years of transactions conducted through the payments systems to address Elon Musk's allegations about "fraudulent payments" being made by Treasury. U.S. Senators Elizabeth Warren (D - Massachusetts) and Ron Wyden (D - Oregon) have pushed for the inspector general office's to launch an inquiry at the Treasury, citing inconsistent information the government has provided about what DOGE is doing with Treasury systems.

"We expect to begin our fieldwork immediately," Inspector General Loren J. Sciurba wrote in a letter. "Given the breadth of this effort, the audit will likely not be completed until August; however, we recognize the danger that improper access or inadequate controls can pose to the integrity of sensitive payment systems. As such, if critical issues come to light before that time, we will issue interim updates and reports."

President Trump, however, has also been pressuring inspector generals to launch investigations in support of his agenda to find fraud in government agencies and has

fired more than a dozen independent inspector generals to, reportedly, remove officials not in alignment with his agenda. This raises concerns about whether the inspector general audit will be allowed to proceed without interference.

Zero Day is a reader-supported publication. If you found this article valuable, you can support my work by becoming a paid subscriber and receiving content that is only available to paid subscribers, in addition to all other content. Or you can subscribe for free to receive more content like this to your inbox. ***And if you know anything about what is going on inside government agencies right now, particularly with regard to DOGE, please contact me on Signal at KimZ.42.***

Iranian Hacktivists Strike Medical Device Maker Stryker in "Severe" Attack that Wiped Systems

Stryker, a leading maker of medical devices, was hit early this morning with a cyberattac…

Mar 11, 2026 · 3 min read · 2 comments

Trenchant Exec Who Sold His Employer's Zero-Day Exploits to Russian Buyer Sentenced to 7 Years in Prison

A former Trenchant executive who pleaded guilty last year to selling his company's…

Feb 24, 2026 · 10 min read · 1 comment