MARKO ELEZ "RESIGNED" THE DAY HIS WRITE ACCESS TO PAYMENT SYSTEMS WAS DISCOVERED

According to the currently operative story, Marko Elez – the DOGE [sic] boy who had source code for Treasury's payments system – resigned in response to a query from WSJ reporter Katherine Long about his social media posts in support of

> A key DOGE staff member who gained access to the Treasury Department's central-payments system resigned Thursday after he was linked to a deleted social-media account that advocated racism and eugenics.
>
> Marko Elez, a 25-year-old who is part of a cadre of Elon Musk lieutenants deployed by the Department of Government Efficiency to scrutinize federal spending, resigned after The Wall Street Journal asked the White House about his connection to the account.
>
> "Just for the record, I was racist before it was cool," the account posted in July, according to the Journal's review of archived posts.
>
> "You could not pay me to marry outside of my ethnicity," the account wrote on X in September. "Normalize Indian hate," the account wrote the same month, in reference to a post noting the prevalence of people from India in Silicon Valley.
>
> After the Journal inquired about the account, White House spokesperson Karoline Leavitt said that Elez had

> resigned from his role.

But that belief is only based on correlation, not any proof of causation. Long asked about posts that are in no way exceptional for the far right boys Elon has infiltrated into the government. And Elez resigned that same day.

Sure, Elon *implied* that Elez quit because the boy's far right ideology was exposed — he led a campaign for his reinstatement. That campaign — and JD Vance's support for it — similarly led a lot of people to believe that Elez *had* been reinstalled at Treasury. But multiple court filings claim that Elez resigned and never came back, at least not to Treasury.

In fact, there are two things that might provide better explanations than the discovery that like Elon himself, Elez is a racist.

As WSJ itself notes, Elez resigned the same day that Colleen Kollar-Kotelly ordered that Elez, then still identified as a Special Government Employee, be granted only read-only access to Treasury's networks. Once Elez no longer worked for the defendants in that case — starting with Scott Bessent — then any access he had would be exempted from the order.

More importantly, as a court filing submitted yesterday reveals, Elez' resignation happened the same day that Treasury discovered Elez's Bureau laptop, "had mistakenly been configured with read/write permissions instead of read-only." The filing is a declaration from Joseph Gioeli, who has been employed as the "Deputy Commissioner for Transformation and Modernization in the Bureau of the Fiscal Service" since 2023 and is a civil servant first hired in the first year of Trump's first term.

His declaration describes how the 4-6 week "payment process engagement plan" initiated (per Thomas Krause) on January 26 required giving Elez risky access to payment systems. Gioeli describes how they tried to mitigate those risks.

> 11. The scope of work as envisioned in the engagement plan required access to Fiscal Service source code, applications, and databases across all these Fiscal Service payment and accounting systems and their hosting environments. This broad access presented risks, which included potential operational disruptions to Fiscal Service's payment systems, access to sensitive data elements, insider threat risk, and other risks that are inherent to any user access to sensitive IT systems. In light of these risks, BFS and Treasury Departmental Office employees developed mitigation strategies that sought to reduce these risks.
>
> 12. These measures included the requirement that Mr. Elez be provided with a BFS laptop, which would be his only method of connecting to the Treasury payments systems, both in connecting with the source code repository and for his read-only access of the systems. He had previously been provided a Treasury laptop from the Department shortly after he onboarded, but due to Bureau security policy, that device was restricted from accessing the BFS systems and services he had requested. BFS used several cybersecurity tools to monitor Mr. Elez's usage of his BFS laptop at all times and continuously log his activity. Additionally, the Bureau enabled enhanced monitoring on his laptop, **which included the ability to monitor and block website access, block the use of external peripherals (such as USB drives or mass storage devices)**, monitor any scripts or commands executed on the device, and block access to cloud-based storage services. Additionally, the device contained data exfiltration detection, which alerts the Bureau to

> attempts to transmit sensitive data types. The laptop is also encrypted in accordance with Bureau policy, which, if the laptop were stolen or lost, would prevent unauthorized users from accessing data contained within the laptop.
>
> 13. Additional mitigation measures that were adopted included that Mr. Elez would receive "read-only" access to the systems, and that any reviews conducted using the "read-only" access would occur during low-utilization time periods, to minimize the possibility of operational disruptions. While providing a single individual with access to multiple systems and data records accessed here was broader in scope than what has occurred in the past, this read-only approach is similar to the kind of limited access the Bureau has provided to auditors for other Treasury non-payment systems, though even in those scenarios the availability of production data was significantly limited. [my emphasis]

Gioeli goes on to describe how, starting on February January 28, the Bureau gave Elez source code in a sandbox environment.

> 16. On January 28, 2025, the Bureau provided Mr. Elez with the **Bureau laptop and with copies of the source code** for PAM, SPS, and ASAP in a separate, secure coding environment known as a "secure code repository" or "sandbox." Mr. Elez could review and make changes locally to copies of the source code in the cordoned-off code repository; however, he did not have the authority or capability to publish any code changes to the production system or underlying test environments. 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. [my emphasis]

Then, *six days after* giving him that sandbox access, *using the same laptop*, they gave him read-only access to first two and then one more systems.

> 17. On February 3, 2025, consistent with the engagement plan and mitigation measures developed, Mr. Elez was provided with read-only access, **through his Bureau laptop**, to the certain BFS systems. The read-only access that Mr. Elez was provided gives the user the ability to view and query information and data but does not allow for any changes to that information and data within its source system. While this reduces risk, it does not fully eliminate the risks identified in the assessment (for example, the risk of overburdening the system with a complex read-only query). Specifically, Mr. Elez was provided read-only access to the Payment Automation Manager (PAM) Database, Payment Automation Manager (PAM) File System, and, subsequently on February 5, the Secure Payment System (SPS) Database.

After he got that access, per a review of the logs, Elez copied some files from the active database onto his Bureau laptop, on which he had the source code.

> 18. ISS configured his network access and assisted him in setting up the necessary tools to connect to the PAM database on February 3. His access was closely monitored by multiple BFS administrators throughout the process on February 3. That same day, he received a “walk-through” demonstration of two BFS

> payment systems, the PAM database and the PAM file system (the system that controls the payment file "landing zone" discussed above), to see how the systems worked. He logged in with his read-only access to these systems on February 3 during this "walk-through" demonstration. **The Bureau is in the process of reviewing the logs of Mr. Elez's activity on his Bureau laptop**, and this review remains ongoing. Based on the preliminary log reviews conducted to date, it appears that on February 3, Mr. Elez **copied two USAID files directly from the PAM database to his BFS laptop**; on February 4 and 5, Mr. Elez accessed the PAM file system; and on February 5, Mr. Elez accessed the PAM payment processing database. These activities are consistent with the read-only access that Mr. Elez was provided and did not change or alter any BFS payment system or record within their source systems. As noted, **reviews of Mr. Elez's work are still actively occurring**; I do not have any more detail to provide at this time about his activities with respect to PAM. [my emphasis]

Then, on February 5, Elez got access to the payment system itself — again, with the same laptop on which he had source code.

> 19. Due to scheduling constraints, Mr. Elez was unable to meet with Bureau personnel to set up his access to the SPS database until February 5. On that date, lSS held a virtual walk-through session to help him to connect to the SPS database. He accessed this database exclusively under the supervision of Bureau database administrators in a virtual walkthrough session. According to the preliminary review of logs the Bureau has conducted to date, it appears Mr. Elez accessed the SPS database only

> once during that walk-through demonstration on February 5. It does not appear that he accessed the database again. As part of the ongoing review, **additional log reviews are currently underway to confirm this**. Mr. Elez never logged into ASAP, CARS, or ITS.gov, as technical access to those systems was never established for him. [my emphasis]

The next day, "it was discovered" (Gioeli does not say by whom, which means we're not seeing a declaration from that person) that Elez actually "had mistakenly been configured" with read/write access, rather than "read only."

> 20. On the morning of February 6, it was discovered that Mr. Elez's database access to SPS on February 5 **had mistakenly been configured with read/write permissions instead of read-only**. **A forensic investigation was immediately initiated** by database administrators to review all activities performed on that server and database. The initial investigation confirmed that all of Mr. Elez's interactions with the SPS system occurred within the supervised, walk-through session and that no unauthorized actions had taken place. His access was promptly corrected to read-only, and he did not log into the system again after his initial virtual over-the-shoulder session on February 5. To the best of our knowledge, Mr. Elez never knew of the fact that he briefly had read/write permissions for the SPS database, and never took any action to exercise the "write" privileges in order to modify anything within the SPS database—indeed, he never logged in during the time that he had read/write privileges, other than during the virtual walk-through — and forensic analysis is currently underway to confirm this. [my emphasis]

Throughout his declaration, Gioeli stresses that *they're still investigating* whether Elez did something unauthorized with his access.

> 21. As noted above, the Bureau used several cybersecurity tools to monitor Mr. Elez's usage and continuously log his activity. While forensic analysis is still ongoing, Bureau personnel have conducted preliminary reviews of logs of his activity both on his laptop and within the systems and at this time have found no indication of any unauthorized use, of any use outside the scope that was directed by Treasury leadership, or that Mr. Elez used his BFS laptop to share any BFS payment systems data outside the U.S. Government.

And his declaration stops short of saying that some mitigation techniques were used. For example, Gioeli says that the enhanced monitoring on Elez' Bureau laptop had the ability to "block the use of external peripherals (such as USB drives or mass storage devices)" and access to the cloud, but it doesn't say whether those functionalities was used.

Plus, Gioeli's declaration makes it clear that they have't involved Elez in any review of his access. No one has asked Elez, for example, whether he knew he had write access to the payment system.

Similarly, in an earlier declaration submitted in the parallel DC case, Thomas Krause gave a very couched answer about whether Elez had has any ongoing access.

> I currently have no reason to believe Mr. Elez retains access to any BFS payment data, source code, or systems."

Did anyone think to ask the guy? Does anyone know where that guy is? Are you going to interview him? Or is someone deliberately trying

to keep him from being questioned further?

Worse still, Thomas Krause declaration submitted in the NY case doesn't even say that Elez has left Treasury — only that he has resigned from the role of, "working closely with engineers at the Bureau of the Fiscal Service (BFS) on information technology (IT) matters in service of BFS's mission to promote financial integrity and operational efficiency of the federal government through accounting, financing, collection, payment, and other relevant BFS services."

> On February 6, 2025, Mr. Elez submitted his resignation from this role. On that same day, he turned in his Treasury laptop, BFS laptop, access card, and other government devices; his BFS systems access was terminated; and he has not conducted any work related to the BFS payment systems since that date.

Elez was made a Treasury employee — contrary to early reports, he was not a SGE. That may make it easier to shuffle him off somewhere else.

What Gioeli describes is the panic that ensues when a guy who had high level access quits unexpectedly. And to date, we've never been given a formal explanation of *why* he quit — or whether he was asked to do so. We certainly can't reconcile the claims that he has been reinstated with claims that he's not doing what he was doing at Treasury.

Everyone has always assumed that Elez quit because his racism was discovered. But given the timeline, we can't rule out that he quit because of the access concerns (and ongoing investigation) at Treasury.

Timeline

January 21: Elez hired.

January 23: Krause hired.

January 26: Treasury focuses on USAD. Treasury also adopts a 4-6 week engagement plan.

January 28: Bureau provides Elez with Bureau laptop copies of the source code for PAM, SPS, and ASAP in sandbox.

January 31: Treasury focuses on TAS codes; Elez assists in "automating" manual review of payments. "A high-ranking career official at Treasury also raised the issue of risks from DOGE access in a memo to Treasury Secretary Scott Bessent."

February 3: Treasury gives Elez access to PAM. Booz threat contractor delivers report warning of grave insider threat.

February 5: Treasury gives Elez access to SPS, the payment system.

February 6 (afternoon): Elez resignation.

February 7: Treasury flags but then approves four payments. WaPo publishes story about Booz report and Booz contractor is fired.

February 8: Paul Engelmeyer limits Krause's access.

February 10: Millenium Challenge Corporation submits, but then requests not to process, a payment.

Documents

Opposition to Stay

Thomas Krause Declaration: Describing the plan to use technology to provide more oversight over payments (citing three Biden-era GAO reports, not anything DOGE has discovered).

Vona Robinson Declaration: Describing that the only payment that has been intercepted at Treasury was a payment to the Millenium Challenge Corporation.

Michael Wenzler Declaration: Describing the hiring, employment status, revisions thereof, of

Thomas Krause and Marko Elez, and also confirming Elez' resignation *from Treasury*.

Joseph Gioeli Declaration: Describing the circumstances of Elez' access and the investigation into what he did with it.