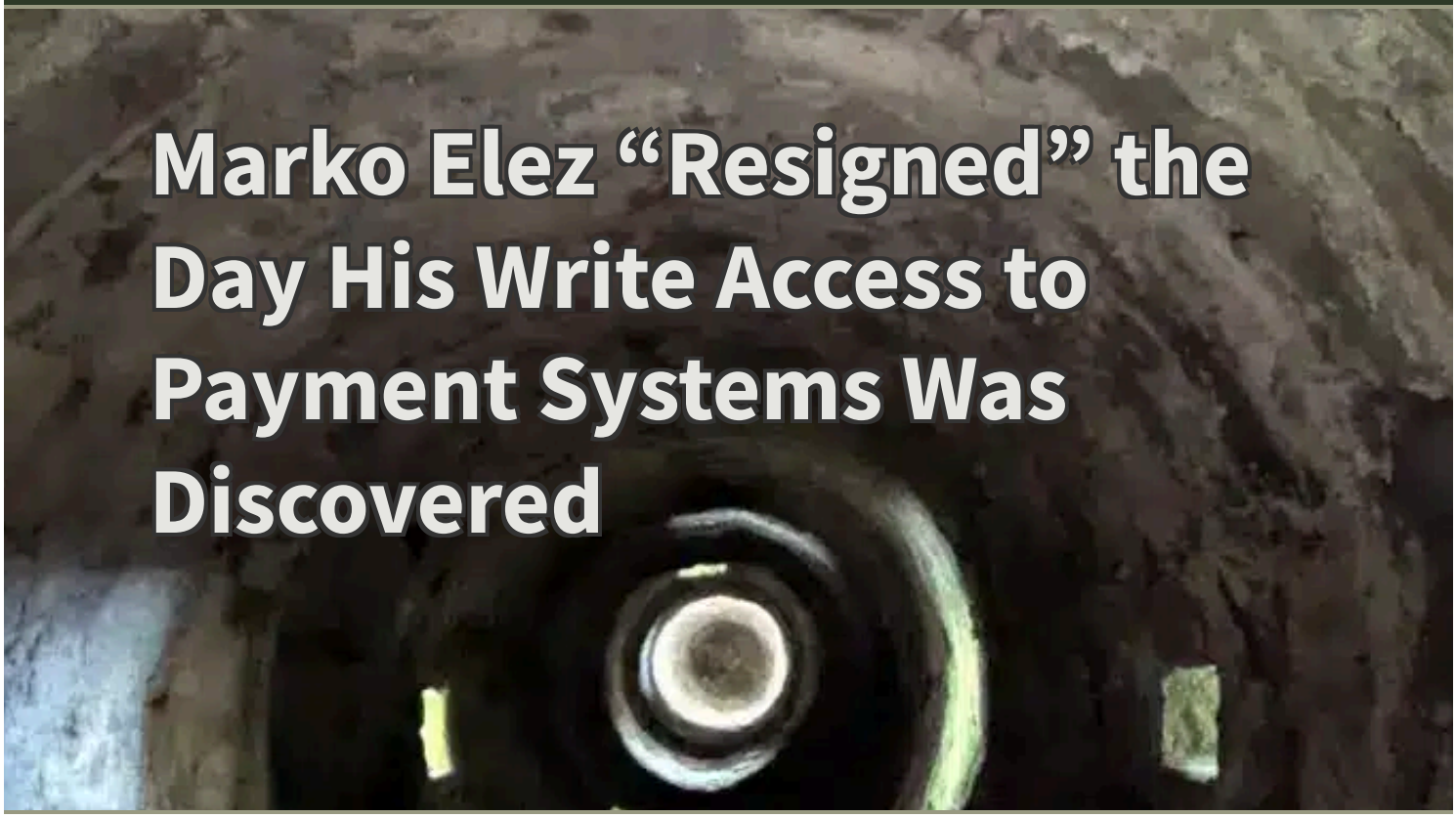

Marko Elez “Resigned” the Day His Write Access to Payment Systems Was Discovered

by emptywheel | Feb 12, 2025 | in 2024 Presidential Election, in DOGE, in Trump 2.0 | 41 comments

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.

Tags: Colleen Kollar-Kotelly, Deryl Paul Dedmon, Jeanette Vargas, Marko Elez, Scott Bessent, Thomas Krause

← **"The Fraudsters Complain the Loudest and the Fastest:" Legacy Media Ignores Import of Gaza Condom Fact Check**
Thomas Krause Says Trump Had to Close USAID because of Trump's Poor COVID Management →

41 Comments

charlie_on_the_MTA on February 12, 2025 at 9:44 am

So on February 3, he took all file with all USAID payments and made a copy.

1. Who gave him that order?
2. What was done with that information?
3. Did he have authority to copy and disseminate that information?

James White_12FEB2025_0959h on February 12, 2025 at 9:59 am

Something for you to look into and perhaps ask Congresspeople about. Congress has the power of the purse via the Constitution as you well know but they also have other powers. Art. I, Sec. 8, Cl. 15: Congress has the power to call forth the Militia to execute the laws of the Union and suppress Insurrections. The Insurrection Act empowering the President is irrelevant to Congress' power, that act did not change the Constitution. Elon & crew and the President are driving a full insurrection now.

[***Welcome to emptywheel****. Please choose and use a* ***UNIQUE*** *username with a* ***minimum of 8 letters****. We have adopted this minimum standard to support community security. Because username "James White" is too similar to a contributor'*

name it will be temporarily changed to match the date/time of your first known comment until you have a new compliant username. Thanks. /~Rayne]

charlie_on_the_MTA on February 12, 2025 at 10:07 am

I'd focus on Jan 26 and Jan 27.

Per timeline, on Jan 26 Treasury started process on flagging USAID payments.
"Specifically, the Bureau was directed to develop a process to
identify all USAID payment files within the PAM file system's "landing zone," to flag those payments for the State Department as potentially implicated by the President's
foreign aid Executive Order, prior to their entry into the PAM payment processing systems."

On Jan 27, Treasury was told that State would block all payments.

From the politico story,

"
On Monday morning, Jan. 27, Marocco arrived at USAID headquarters with more than a dozen people, most, if not all, representatives of the Department of Government Efficiency, the Trump-blessed initiative run by tech mogul Elon Musk seeking to shrink the federal government, according to the five people."

Again who is giving the order here? Marocco apparently blew up on the 23rd when he found USAID had sent out $153M in salaries.

> **emptywheel** on February 12, 2025 at 12:45 pm
>
> I deal with Marocco's usurpation of Rubio's role here.
>
> https://www.emptywheel.net/2025/02/11/donald-trump-incorrect-shell-game-of-appropriated-spending/
>
> But I agree I need to merge all these timelines.

T.F._12FEB2025_0045h on February 12, 2025 at 10:21 am

Other bits worth adding to your timeline:
January 24. Rubio orders funding freeze to USAID contractors.
January 26. Treasury BFS approves a process to stop USAID payments by flagging them in the PAM file system "landing zone"
January 26. Rubio publicly announces a "pause" of all foreign aid thru the State Department or USAID
January 27. State Department stops USAID payments prior to them being submitted to Treasury. 56 senior USAID officials are placed on leave and escorted out by law enforcement, for suspicion of not going along with the funding freeze.
January 31. Treasury's top career civil servant, David Lebryk, is placed on leave and resigns for refusing to go along with DOGE's requests for payment systems access
February 1. USAID web site is taken down.
February 2. Musk tweets about DOGE shutting down payments and that he is feeding USAID to the wood chipper.
February 3. Rubio is announced as acting admin of USAID and employees are told not to report to work
February 4. Treasury Department sends a misleading letter to congress, saying that there has been no rejection of payments and that the Krause-led DOGE team has read-only access for "operational efficiency assessment"
February 5. DOJ lawyers incorrectly report to a judge that Elez is a SGE and has only read-only access to Treasury systems
February 7. USAID website announces all personnel are on administrative leave globally
February 11. DOJ filing reports the factual error about Elez's hiring status. Above-linked declarations made and signed.

[***Welcome back to emptywheel***. *SECOND REQUEST: Please choose and use a* ***unique*** *username with a* ***minimum of 8 letters****. We have adopted this minimum standard to support community security. Because your username is too short it has been temporarily changed to match the date/time of your first known comment until you have a new compliant username. Until you change your username your comments will continue to go into moderation for manual clearance. /~Rayne*]

crankyOldGuy on February 12, 2025 at 10:26 am

Good discussion, thank you.

I have never been a DB admin, but I have worked with them for years on highly sensitive corporate DB's.

First, this is a top-level payment system, not a place where decisions are made about how and where to spend money. Security requires the two functions be kept completely separate. So there is no valid reason for MuskmElon's crew to be poking around in the name of government efficiency. But if your goal was a complete forcible government shutdown, you came to the right place. I'm pretty certain someone around MuskmElon is savvy enough to know this, though his college crew may not.

It isn't really a surprise that someone got the wrong access level…it's happened to me in the past. But under the circumstances, it is quite reasonable to suspect ulterior motives. And of course, why did he suddenly drop out of sight?

P J Evans on February 12, 2025 at 11:27 am

I had access to the workstations of all the engineers in the company, because I was doing QC on the graphic-data systems and sometimes had to hunt down stuff. When I left for a year, that access wasn't revoked, so I still had it later when I was working with GIS. I had more access than my immediate boss!

dopefish on February 12, 2025 at 2:59 pm

crankyOldGuy wrote:
"First, this is a top-level payment system, not a place where decisions are made about how and where to spend money. Security requires the two functions be kept completely separate."

Definitely. But perhaps DOGE was just trying to create a way to "scan the stream of outgoing payments" in order to detect (perhaps with AI or whatever) payments they don't like–such as payments they might ideologically believe to be "waste, fraud or abuse".

Since all payments ultimately go through the Treasury, perhaps their goal was to detect occurrences of "bad payments" so they could then go to the source agencies and fire the people and shut down the programs which were originating those payments. (I couldn't guess whether there's actually

some way of doing that that actually complies with all applicable laws, such as privacy laws)

Alternatively, perhaps they really were (are?) taking a giant shortcut and just trying to add a technical means to Treasury's systems to let them just block any "bad payments" from going out. That sounds both technically and legally risky, but this administration might not care.

PeteT0323 on February 12, 2025 at 10:34 am

This makes me ill.

This is a major nit, but it torques me none the less. I've been out of the biz quite a while, but typically I have to wonder that devices (laptops) are not configured for read or read/write access. Login accounts are. But I could be wrong…

====
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."
=====

There is not an IT (security) professional worth their salt that would condone this and should have resigned on the spot when ordered to do this. Apparently I am wrong again.

neetanddave on February 13, 2025 at 1:34 am

yeah, that stuff is done at a user level, not machine level. surely to God they didn't have them using a "guest"-type login that had Lord knows what access…

Boycurry on February 12, 2025 at 10:34 am

Great post but somehow we are still missing the forest for the trees. Why would he need access to the code (read only or otherwise) at all to find "government waste"? This is the question that needs to be asked by a court or by the press. Is it the

programming language itself that is inefficient? Of course this is to insert backdoor code to turn off funding for blue states or enemies or anyone that they will choose to extort. The basic code access premise is the issue, not whether he had read only access or was just in his sandbox perfecting his attack method.

dopefish on February 12, 2025 at 2:11 pm

He needed to be able to read the code, in order to figure out a little bit about how it worked and thus to figure out how to interpret the various records that he could read from the production databases (using his read-only access).

Also, he was probably tasked with developing a modified version of the code that would enable DOGE (or some other politically-reliable Trump admin figure) to block certain payments from occurring. <a href="https://www.politico.com/news/2025/02/08/elon-musk-doge-government-payments-014920"There was some reporting a few days ago that DOGE convinced the Treasury to agree that “all outgoing government payments” would now have a “payment categorization code” for auditing purposes. This was a new field (or an existing field repurposed for this usage?) that would be added to all of the payment requests coming to Treasury from the other government agencies. In that article, Musk was described as saying they were “not yet applying ANY judgment to this rationale” but that all payments must have one. So it seems entirely possible that Elez (modifying his copy of the code in his self-contained sandbox machine) may have been preparing code changes related to auditing this new field, searching for payments with certain descriptions in this field, or perhaps blocking payments with certain descriptions in this field. Those code changes were (apparently) only in his self-contained sandbox machine and Elez did not have the technical access to make code changes on the real production systems; that would have to be done by others who do have that access. (And of course one hopes they would very carefully review his code changes before ever doing that.)

earlofhuntingdon on February 12, 2025 at 2:19 pm

Too many assumptions for my taste, too much credulity about what a DOGE [sic] hacker intended to do with a live govt system.

> Musk, for example, is a bigger liar than Trump, which would make his characterizations of what he intends and is doing unreliable.
>
> And the last three weeks demonstrates that what DOGE [sic] and Trump are doing does not involve “persuading,” whether it’s Treasury or anyone else. It’s ordering.

> **dopefish** on February 12, 2025 at 6:45 pm
>
> Yes, those are fair points.
>
> I guess I now feel the chance of “accidental destruction of global economy due to idiot clownshow tampering with Treasury computers” is lower than I previously feared (though probably not zero).
>
> The likelihood that some combo of Trump/Musk/DOGE is attempting to leverage Treasury systems in an undemocratic and maybe-illegal way, seems as high as ever.

Error Prone on February 12, 2025 at 10:50 am

Without reading detail of the listed items, the question occurs, did Eliz have access to the device only at Treasury, the device always in their building and custody when Eliz was elsewhere, or did he have after hours capability, at home, to continue working? And clearly “could block USB usage” begs more detail. “Could” and “did” or “never did” are different wordings.

Whether the logs might show irregular hours, as many tech people keep, is unclear. From the excerpting, as, again, I did not study any of the referenced documents. Just seeing some unclear things from the text excerpted in the post. The main thing, did Eliz keep personal custody of the assigned device, ever, away from Treasury offices, or did he have to check it out from Treasury custody and access it only at Treasury’s offices during regular hours?

Error Prone on February 12, 2025 at 10:58 am

When Eliz had custody and use of the laptop, was he allowed cell phone access to numbers outside of the Treasury Dept? If so, were his call details logged or monitored?

Bob Tetrault on February 12, 2025 at 11:19 am

Thank you. This blows away my MITM thesis of yesterday. And yes, source code? Really? That's an attack posture.

P J Evans on February 12, 2025 at 11:28 am

What would a computer guy know about fraud and waste? That's the first question.
The second is, why is he getting access to those systems at all?
And who died and made Musk president?

Rayne on February 12, 2025 at 12:10 pm

Musk could not become president no matter who died. This situation must chap Ted Cruz's ass.

P J Evans on February 12, 2025 at 1:56 pm

Should have tagged that as snark – it's a common line, usually as "who died and made you [king/god/boss]?"

Rayne on February 12, 2025 at 7:37 pm

But it's literally the problem — Musk has become the de facto president.

earlofhuntingdon on February 12, 2025 at 9:20 pm

That was very much the message from the body language at that Musk, Musk toddler, toddler Trump presser.

depressed Chris on February 13, 2025 at 10:51 pm

I would donate a fair amount of my retirement account to personally chap Ted Cruz's ass. I'd even spring for the cat o nine tales.

Boycurry on February 12, 2025 at 12:11 pm

The Republican party

originalK on February 12, 2025 at 11:57 am

I know part of the Emptywheel secret sauce is the time difference, but this is an amazing report. While on the one hand, the declaration shows how much security and oversight were directed at Elez's activities (while still complying with the directives of the administration), you have pinpointed where it went off the rails.

For anyone who isn't going to read the declaration, I would just add this about the SPS system (taken from it):

> SPS is a system through which paying agencies securely create, certify, and submit individual payment files to Treasury; it is also typically used for one-time large dollar amount transactions.

My follow-up questions are – is this declaration supposed to favor the plaintiff or the defendant? Why was it produced/what purpose is it supposed to serve?

Matt Foley on February 12, 2025 at 12:47 pm

Now that you mention it, yeah, it seems unlikely that a MAGA techbro resigned out of shame for his racism.

drhester on February 12, 2025 at 1:28 pm

Nathan Tankus has an apropos post today. He's very good at this.
https://www.crisesnotes.com/bombshell-court-filings-confirm-wired-notes-on-the-crises-reporting-raise-alarms-about-bfs-based-impoundment/

Max404Droid on February 12, 2025 at 7:08 pm

Everyone: this piece by Nathan Tankus is a MUST READ. They are trying to implement a system whereby they can filter any payments at a very granular level for non-payment. Micro-impoundments so to speak, under the radar and nearly impossible to observe – until the funds mysteriously do not arrive. The possibilities for co-opting cronies of the dictator are breathtaking.

Ginevra diBenci on February 13, 2025 at 10:57 am

Hey y'all, Dr Hester has given you a link to the goldmine–if the goldmine is the closest approximation of a finance reporter's informed perspective on what the ElonElez brigade has gotten up to with YOUR money.

Max404Droid calls it a "MUST READ." To that I say 'ditto.'

"Mr. Elez assisted in automating the manual review of the payment files." To wit, this (*their* words, not Tankus's or mine) dizzying double-speak in a description of how that wrench got thrust into the gears of USAID via the State Department. Fuckery? Maximum. Accountability? Zero. Zed. Null set.

earlofhuntingdon on February 12, 2025 at 2:07 pm

If you're giving a newbie, with a reputation as an unprincipled hacker, a laptop with sandboxed access to sensitive source code, why would it not be air-gapped, with no access to live systems? The "disclosures" here are a little too clever by half.

Ginevra diBenci on February 13, 2025 at 11:01 am

Nathan Tankus thinks so too.

Having wondered if I (more a linguistic than a tech person) had made a fool of myself squawking about this here, I was relieved to find that an expert

like Tankus also found their protestations suspect.

dopefish on February 12, 2025 at 2:41 pm

Actually, this new information from Joseph Gioeli III's declaration is the most reassuring thing I've read since the beginning of this whole mis-adventure. If this declaration is truthful and accurate, it sounds like Elez did not have the ability to deploy his modified code into the "real" production environment; that would probably have to be done by a senior civil servant at Treasury who did have that access.

It sounds like the BFS laptop they gave him was properly secured and was properly configured so that any access Elez made to mission-critical production systems was monitored and could be properly audited. His laptop "sandbox" contained a copy of the code so he could study and experiment with that code to learn something about how parts of it worked, and (presumably) so he could develop and test some sort of modifications to the code.

But he could only modify his own copy of code "in the sandbox" (i.e. on that BFS laptop) — it sounds like he was not given any technical ability to modify code on the mission-critical "production" systems. They did give him the ability to read sensitive data *from* some mission-critical systems, perhaps so that he could test his modified code by feeding some real-world data through it.

It seems plausible that he was tasked by DOGE to prepare some sort of code changes to help them "detect waste, fraud and abuse" (ha ha) among the payments… perhaps his changes had something to do with the new "payment categorization code" field that Musk talked about a few days ago, or perhaps he was working on something altogether different.

(Here's one totally hypothetical scenario: Suppose DOGE wanted to train an AI model to detect "suspicious" payments and flag them for human review. In that scenario, perhaps Elez was developing some sort of "conversion function" that could take a payment record as input and convert it into a different format that was easier for the AI to operate on. Or perhaps he was actually training a miniature version of the AI on his laptop and then testing it on some "real" data retrieved with

his read-only access, in order to see how this miniature AI performed at some recognition task, such as spotting all USAID payments or whatever.)

Anyway, we don't know exactly what they were doing and it might still have been risky in various ways (impossible for us to know for sure), but the whole thing might not have been as crazy as some of last week's leaks suggested. I might be able to get a good night's sleep for the first time since this story broke.

The early leaks gave an impression that Elez might be making code changes directly on production systems with no auditing or oversight, which would have been totally insane. But Joseph Gioeli III's declaration gives the impression there actually was some adult supervision going on and that Elez had no ability to change the real code in production. There may still be questions about whether any sensitive production data was copied off of his BFS laptop or not, etc.

Edit: I know this comment is too long, apologies!

kpavlovic on February 12, 2025 at 2:48 pm

You should read the Tankus explanation at the URL in drhester's comment above.

Ginevra diBenci on February 12, 2025 at 4:43 pm

Sorry, dopefish, but I don't find Gioeli's declarations reassuring. He seems to snow us with competent-sounding detail, only to sneak in sucking gaps where the gist should be.

"It was discovered"? Give me a break. Surely even he must have heard the echo of "Mistakes were made." Because mistakes WERE made.

How is it that Elez is described as doing nothing without oversight, and yet "investigations" into what he actually did remain ongoing? What were his overseers ("over the shoulder") doing, anyway?

dopefish on February 12, 2025 at 8:20 pm

There are different ways to monitor someone's activity. Sitting next to them and watching them work might be one kind of "oversight"

(although that “over the shoulder” phrase is used to describe Krause, who was not granted his own computer access but would sometimes see things on Elez’s screen).

Security employees reading through audit logs that had been recorded by the computer as Elez worked, to carefully confirm–after the fact–that he didn’t do anything malicious, is a different kind of “oversight”.

Page 7 of the Gioeli declaration also describes how the security group, ISS held a “virtual walk-through session to help [Elez] connect to the SPA database. He accessed this database exclusively under the supervision of Bureau database administrators in a virtual walkthrough session.” Imagine Elez and the DB admins in a Zoom call (or Teams meeting, or whatever the hell they use), with the DB admins showing him what to type, confirming that the queries he wanted to run would not overload the system, and so on.

There are still parts of the story we haven’t heard yet–such as what exactly Elez was working on, which might be something unconstitutional or at risk of insider abuse, etc. (blocking payments?)

I do think Gioeli’s declaration–under penalty of perjury–describes a much more prudent and careful engagement between DOGE and Treasury’s computer systems than the initial news leaks made it seem. Everything in it sounds believable to me, and my fear level about an *accidental* catastrophe there is now much lower.

> **Ginevra diBenci** on February 13, 2025 at 9:22 am
>
> I’m more worried about the deliberate catastrophes myself–the ones whose potential appears to lurk in every gap Gieoli left in his declaration.

earlofhuntingdon on February 12, 2025 at 4:47 pm

Instead of making your comment longer by writing that it's too long, don't apologize for it, shorten it.

dopefish on February 12, 2025 at 6:50 pm

You're right, next time I'll do better.

TomVet475 on February 12, 2025 at 4:36 pm

I really appreciate all the informed discussion of the technical issues here, but want to point out something very basic that no one seems to have caught.

In the blockquote of ¶18, on Feb 3, he copied 2 files from the database to his laptop with read-only privileges; 3 days later (¶20) it was discovered he had read/write ability.

I only have experience as admin of my own Windows devices over 15 or so years, but you cannot copy files from one location to a new location or device with read-only because that entails writing to a new file.

Everything they tell us about this is highly suspect.

originalK on February 12, 2025 at 6:42 pm

Read/write in this configuration would be more akin your windows device being able to download/upload from the internet, a client-server relationship. On the 3rd, he could read the data/files of the PAM system, and download them to the laptop. He couldn't modify the data on the server or upload new files. On the 5th he could do so with the SPS database.

thequickbrownfox on February 12, 2025 at 8:53 pm

Doesn't appear he has a clue about COBOL.

Anyway, have at it coders:

https://github.com/markoelez

emptywheel

Come for the weedy coverage of legal cases, politics, and left theory. Stay for the potty mouth and craic.

support emptywheel

This site's work is possible through readers' support. Choose a support option at the link below.

donate

printer friendly version

font resizer

A A A

recent posts

Seb Gorka Orders Europe to Harbo[u]r His Kind of Terrorists

May 8, 2026

Cole Allen Catalogs Jeanine Pirro's Verbal Diarrhea

May 8, 2026

Kash Patel Changes His Mind about Sarah Fitzpatrick's Sources

May 8, 2026

The Loaner AUSAs Todd Blanche Disavows

May 7, 2026

Trump's Base Motives

May 7, 2026

recent comments

Savage Librarian on Seb Gorka Orders Europe to Harbo[u]r His Kind of Terrorists

Rugger_9 on Seb Gorka Orders Europe to Harbo[u]r His Kind of Terrorists

Ginevra diBenci on Trump's Base Motives

Ginevra diBenci on The Loaner AUSAs Todd Blanche Disavows

Attygmgm on Seb Gorka Orders Europe to Harbo[u]r His Kind of Terrorists

emptywheel

information

About
Community Guidelines

connect

Sign Up
Contact
Support

all categories **special projects**

Copyright © 2026 emptywheel. All rights reserved.

Comment Policy | Privacy Policy