DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

COMMISSIONER

March 2, 2022

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Maloney:

Thank you for your letter dated February 11, 2022. You expressed concern about the IRS's partnership with a credential service provider (CSP) using facial recognition to authenticate the identity of people creating new online accounts. As you are aware, on Monday, February 7, 2022, the IRS announced its transition away from these processes. We still wanted to respond to your letter and provide additional detail on the ways in which we are focused on securing taxpayer data, protecting taxpayer privacy, and ensuring broad-based and equitable access to our online tools.

Identity Theft and Taxpayer Protection Concerns
The IRS has an unwavering commitment to the protection of taxpayer returns and return information. Protecting taxpayer returns and return information against unauthorized access is a fundamental IRS principle.

Additionally, applicable laws and regulations require certain authentication standards for access certain types of information. National Institute of Standards and Technology (NIST) 800-63-3, Digital Identity Guidelines, establishes the level of authentication and security controls necessary to access various types of information.[1] Also, Office of Management and Budget (OMB) M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, details how agencies should conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access controls.[2] For remote identity proofing, NIST requires a "physical or biometric comparison of the photograph on the strongest piece of evidence to the applicant" or "a biometric comparison between information on the evidence and a biometric characteristic obtained from the applicant."

Our commitment to the protection of taxpayer information can sometimes conflict with our desire to ensure taxpayer access to their own information. Cybercriminals frequently

[1] NIST Digital Identity Guidelines are available at: NIST SP 800-63 Digital Identity Guidelines
[2] OMB Memorandum 19-17 is available at: Office of Management and Budget (OMB) M-19-17

exploit vast amounts of data from breaches outside the tax system to attempt refund fraud. With so much information available online, traditional identity verification methods using "something you have," such as a token, or "something you know," such as a password, are no longer sufficient. We require online authentication methods to ensure data is disclosed only to the relevant taxpayer and to comply with applicable laws and regulations, but we realize these methods can also create difficulties for taxpayers.

Because of these considerations, the IRS moved to facial recognition technology to improve authentication methods. It also needed this technology to comply with current federal standards and guidance for data protection and privacy.

Going forward

We recognize legitimate concerns about the use of facial recognition technology and CSPs. In light of these concerns, we modified our contract with ID.me and made facial recognition authentication optional. We also required ID.me to delete any data it has previously received, and purge new data on an ongoing basis, as detailed in the enclosure. We will confirm ID.me has complied with these requirements through site visits and quarterly compliance reports.

The IRS will continue to work with its cross-government partners to develop authentication methods that protect taxpayer data and ensure broad access to online tools.

Your letter asked us to respond to specific questions about the IRS's authentication efforts. Please find our responses to your specific questions and a copy of the contract as requested in the attached enclosures.

I hope this information is helpful. If you have questions, please contact me, or a member of your staff may contact Amy Klonsky, Chief, National Congressional Affairs Branch, at 202-317-6985.

Sincerely,

Charles P. Rettig

Digitally signed by Charles P. Rettig
Date: 2022.03.02 12:07:14 -05'00'

Charles P. Rettig

Enclosures (2)

Enclosure

1. **Is the IRS planning to instruct ID.me to destroy the biometric data that has been collected from Americans who have created ID.me accounts?**

   We modified the existing ID.me contract, effective February 17, 2022. The modified contract requires ID.me to destroy all biometric selfies, selfie videos, and video recordings of users it had already received by March 11, 2022. Going forward, the credentialing service provider (CSP) will destroy the video selfie and live video chat recording.[1]

2. **Is IRS planning a follow-up compliance site visit with ID.me to ensure that any biometric data not destroyed will continue to be properly safeguarded?**
   a. **If so, when?**
   b. **If not, why?**

   Yes, the IRS is planning to complete a site visit on March 21, 2022.

3. **What ongoing contractual requirements is ID.me required to meet in order to protect and safeguard the biometric information it has already collected?**

   As described in question 1 above, data ID.me already collected will be destroyed by March 11, 2022.

   On an ongoing basis, contractors must follow the general guidance and specific security control requirements in Publication 4812, Contractor Security Controls, Internal Revenue Manual (IRM) 10.23.2, Personnel Security, Contractor Investigations, and IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance. Publication 4812 and IRMs 10.8.1 and 10.23.2 provide comprehensive lists of all security controls and guidance.[2]

4. **How does ID.me's announcement that users can delete their data affect records retention requirements?**

   The February 17, 2022, contract modification changed the records retention period for ID.me. The modified contract requires ID.me to destroy all biometric selfies, selfie videos, and video recordings of users received under the previous contract by March 11, 2022. ID.me will complete this without user involvement.

---

[1] However, any data previously identified as being fraudulently created or identified by Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations /Government Accountability Office (GAO) as part of an investigation is exempted from this purge procedure until the investigation is completed.
[2] Publication 4812 is available at: https://www.irs.gov/pub/irs-pdf/p4812.pdf. IRM 10.8.1 is available at: https://www.irs.gov/irm/part10/irm_10-008-001r. IRM 10.23.2 is available at: https://www.irs.gov/irm/part10/irm_10-023-002.

5. **Will IRS be notifying its users about the process to delete their data with ID.me?**

   No. ID.me will delete the data itself, so taxpayers do not need to take any action. We will, however, provide notification of the new process to affected taxpayers.

6. **How will IRS ensure, on an ongoing basis, that ID.me does not use data it has collected for unapproved or unauthorized purposes?**

   The modified contract requires ID.me to provide access and proof to the IRS to confirm data it collects is promptly deleted.

   There is a minor exception for data subject to ongoing investigations. Until the investigation is complete, ID.me can retain data:

   - previously identified as being fraudulently created or that has been identified by Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations /Government Accountability Office (GAO) as part of an investigation.

   The IRS has full oversight rights and responsibilities to ensure ID.me meets the contractual requirements. The contract gives the IRS authority to audit/inspect ID.me to ensure compliance, as needed.

   ID.me must provide a quarterly self-declaration confirming all biometric data (including selfies, liveness detection recordings, and associated data) and recorded remote live chat sessions have been deleted. The IRS Contracting Office Representative will review the certification and validate compliance quarterly.

   Additionally, CSPs are subject to a number of requirements to ensure data remains secure. CSPs must receive certification from the General Services Administration in the Federal Risk and Authorization Management Program (FedRAMP), with a "Moderate" Authority to Operate (ATO) under the guidelines in NIST 800-53. This ATO confirms a CSP has met rigorous FedRAMP security requirements. Also, each CSP must pass NIST's Facial Recognition Vendor Test and be independently tested by NIST-accredited laboratories.

Contract terms also explicitly limit the use of any data the CSP receives, processes, or produces during the authentication process. Under the contract, a CSP can only use the information the CSP collects for identity verification and credential management. The CSP may not retain, use, sell, or disseminate copies of data that contain information covered by the Privacy Act of 1974. The CSP generally can't share information with other federal agencies.[3]

7. **How much money has already been expended on IRS's contract for ID.me and how much additional outlays are expected based on performance to date?**

   The IRS spent $86,823,159.90 for ID.me licenses to support the IRS digital identity platform. The IRS does not expect any additional outlays this fiscal year based on current usage trends.

8. **How much will it cost to withdraw from or terminate the contract?**

   The IRS has already modified its contract with ID.me as described in this document. There were no costs to modify the contract. Should the IRS choose to terminate the contract in the future, our contract allows for that without additional costs imposed.

9. **What IRS alternatives are being developed to ensure that identity theft is addressed while respecting privacy, security, and equitable access to government services, and when will these alternatives be available?**

   As of the February 21, 2022, contract modification, ID.me now provides an opt-out for the "video selfie" and its use of algorithmic facial recognition. Taxpayers who opt-out can, instead, conduct a live video chat with a trusted referee. This data is subject to the deletion rules described in Question 6. At the same time, the IRS is urgently working with GSA to resolve problems that prevent Login.gov from meeting the IRS's needs.

---

[3] The contract modification states: ID.me will maintain all biometric data (including selfies, liveness detection recordings, and associated data) identified during its normal course of business as being suspicious or potentially fraudulent and will make a report available to IRS and TIGTA of suspicious activity volumes relating to initially issued IRS credentials before the end of the following business day using the reporting process currently in use at IRS. ID.me will maintain all biometric data (including selfies, liveness detection recordings associated data) identified by the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations /Government Accountability Office (GAO) as being necessary in the performance of the responsibility of the Inspector General under 5 USC appendix, to conduct and supervise audits and investigations and to promote economy, efficiency, and effectiveness in the administration of, and to prevent and detect fraud and abuse in and relating to the programs and operations of the Department of the Treasury and the Internal Revenue Service.

Before the IRS can use Login.gov to meet IRS authentication requirements, it must:

- comply with the NIST requirements for Level 2 data security;
- offer the necessary customer service, such as live support options and multilingual options;
- have the technology capacity and performance to support IRS needs; and
- meet other security, fraud, and data protection requirements.

Once these issues are resolved, the IRS plans to immediately begin using Login.gov to authenticate taxpayers.