epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Financial Crimes Enforcement Network, Department of the Treasury

Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement

89 Fed. Reg. 22,231

May 28, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Financial Crimes Enforcement Network's (FinCEN) Request for Information on changing the Consumer Identification Program (CIP) Rule to allow banks to obtain full Social Security Numbers (SSN) from third-party identity verifiers.[1] Under the current CIP Rule, banks must collect a full social security number from every customer when the customer opens a new account. FinCEN's proposal would allow banks to collect only a partial SSN, the last four digits, along with biographic information, and obtain the full number from a third-party service checking the customer's name, biographic information, and partial SSN against a database.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC works to protect privacy by

[1] 89 Fed. Reg. 22931.

advocating for strong, privacy protective standards when individuals interact with corporations and government agencies, including identity verification.[2]

EPIC urges FinCEN to 1) take all possible steps to reduce collection of SSNs online, 2) permit banks to obtain SSNs from third-party verifiers but not permit banks to collect other biographic information, 3) require strong data minimization and data deletion requirements for banks and third-party verifiers, and 4) refrain from encouraging banks to use biometrics for identity verification.

I. FinCEN should take all possible steps to minimize SSN collection online.

In response to 3(a), (d)

The Social Security Number has lost much of its value as a personal identifier. For nearly 20 years, federal policy has aimed to minimize collection and storage of SSNs across agencies, recognizing the extreme risks of a data breach exposing SSNs. Unfortunately, that federal policy has not been successful, and many agencies continue to collect SSNs. Corporations across industries have been even more negligent, collecting SSNs regardless of necessity because the SSN is a convenient signifier of identity. As a result, consumers now regularly disclose their SSNs online, and SSNs are regularly exposed in massive data breaches. In addition to mounting data security risks, the collection of SSN is becoming less effective, as it is no longer a strong signifier of identity. In other words, when someone who submits a matching name and SSN to validate their identity, that is no longer strong evidence that the submitter is the person they claim to be. FinCEN has an important role to play in deprecating the use of SSNs for identity verification to prevent further fraud and identity theft. Allowing banks to collection partial SSNs is an important start.

[2] *See e.g.* EPIC, Coalition Comments to DHS on Advance Passenger Information System: Electronic Validation of Travel Documents (Apr. 3, 2023), https://epic.org/wp-content/uploads/2023/04/IDP-APIS-comments-3APR2023.pdf; EPIC Comments to OSTP on Digital Assets Request for Information (Mar. 6, 2023), https://epic.org/documents/comments-of-epic-to-ostp-on-digital-assets-request-for-information/; EPIC Comments to GSA on Fraud Controls on Login.gov (Dec. 21, 2022), https://epic.org/documents/epic-comments-modified-system-of-records-notice-for-login-gov/; EPIC Spotlights Pondera's Fraud Detection Algorithms for Public Benefits (Jul. 5, 2022), https://epic.org/epic-spotlights-ponderas-fraud-detection-algorithms-for-public-benefits/.

Current OMB guidance and White House policy dating back to 2007 both instruct federal agencies to minimize collection and storage of SSNs. The federal government recognized that agencies collecting SSNs posed a threat and specifically instructed agencies to a) eliminate unnecessary use of SSNs and b) explore alternatives to the SSN.[3] However, agencies have not made enough progress in reducing or eliminating use of the SSN to validate identity. In 2017 the Government Accountability Office (GAO) surveyed federal agencies collecting SSNs, finding that 22 agencies used the SSN in the provision of benefits and services.[4] The GAO issued five recommendations to the Office of Management and Budget to harmonize federal policy and meaningfully reduce how often agencies collect SSNs. As of 2021, OMB could not confirm that it had implemented any of the GAO's recommendations.[5] In short, agencies are repeatedly failing to act to remove the SSN from identity proofing.

Meanwhile, corporate collection of SSNs has skyrocketed. The federal government bears much of the initial responsibility for this trend by requiring banks to collect SSNs under the Bank Secrecy Act of 1970, which would become the CIP Rule, and other regulations.[6] From the 1990s on, companies increasingly used the SSN as a means of identity proofing. Instead of using it to keep track of customers, the SSN is now often used to verify a customer's identity.[7] The financial services industry widely uses the SSN as a universal password, leading consumers to disclose their SSNs

[3] OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf.
[4] GAO-17-553, Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display (Jul. 25, 2017), https://www.gao.gov/products/gao-17-553.
[5] *Id*.
[6] Kenneth Donaldson Meiser, Opening Pandora's Box: The Social Security Number from 1937-2018 at 22 (2018) (master's thesis, UT Austin), https://repositories.lib.utexas.edu/server/api/core/bitstreams/11898164-300c-4243-8fb8-3aaf9862afef/content (arguing that the mandate for banks to collect SSNs facilitated their use in financial services like credit reporting).
[7] *Id.* at 27-29.

regularly online.[8] And with no general data privacy law, companies have cavalierly collected, stored, and disclosed SSNs with insufficient justifications or protections.[9] As a result, the historic regime of using permanent, easily accessible identifiers like the SSN for identity proofing is broken.[10]

The SSN is a weak signifier of identity, and using the SSN in identity proofing creates substantial risks of fraud and identity theft. Data breaches involving SSNs are so common that the SSN has lost much of its value as a signifier that the person providing their social security number is not an imposter. The 2017 Equifax data breach alone exposed the SSNs of more than 145 million Americans.[11] For years, security experts have warned that virtually every person with an SSN has had their number compromised at least once, and that everyone should act as if their SSN has been stolen.[12] A GAO report indicated that past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[13] Yet these harms do not appear on the victim's bank statement or credit report. To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.

Reversing the current state of affairs in which SSNs are freely disclosed and regularly used for identity proofing requires a full-court press, as the White House has recognized. One key aspect

[8] Jonathan J. Darrow & Stephen D. Lichtenstein, *Do You Really Need My Social Security Number - Data Collection Practices in the Digital Age*, 10 N.C. J.L. & Tech. 1 (2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1699184.

[9] Daniel Solove and Chris Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. Ill. L. Rev. 357 (2006), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294.

[10] Marten Lostroh, *Why the Equifax Breach Should Not Have Mattered*, World Congress on Internet Security (WorldCIS) arXiv:1801.00129 (2017), https://arxiv.org/abs/1801.00129.

[11] GAO-18-559, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach at 18-19 (Aug. 2018), https://www.gao.gov/assets/gao-18-559.pdf.

[12] Suzanne Rowan Kelleher, *Everyone's Social Security Number Has Been Compromised. Here's How To Protect Yourself*, Forbes (Aug. 1, 2019), https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=6ea189929ac7.

[13] U.S. Gov't Accountability Off., GAO-14-34, Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent at 11 (2013), http://www.gao.gov/assets/660/659572.pdf.

of that effort is de-normalizing the use of SSNs online. Consumers should not be required to disclose their SSNs, and especially their full SSN, online.

II. Banks should be permitted to collect full SSNs, but not other biographic information, from third-party verifiers.

In response to Question 1 and 2(a).

In contrast to general biographical information, Social Security Numbers are a unique case where banks obtaining partial disclosure from consumers has significant privacy and policy benefits. FinCEN should be careful not to endorse general-purpose data brokering and should not support an industry that has been deeply destructive to privacy while facilitating fraud and identity theft. Therefore, while it is appropriate to seek to minimize the collection of SSNs, allowing banks to rely on third parties (data brokers) as a primary source for more consumer information increases privacy risks to consumers without commensurate benefits.

For more on the specific threats and harms of data brokers see:

- Caroline Kraczon, Data Brokers Threaten National Security. The Consumer Financial Protection Bureau's Fair Credit Reporting Act Rulemaking Can Reduce the Threat, EPIC (Apr. 30, 2024) https://epic.org/data-brokers-threaten-national-security-the-consumer-financial-protection-bureaus-fair-credit-reporting-act-rulemaking-can-reduce-the-threat/

- EPIC, The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better (Feb. 2024), https://epic.org/documents/the-state-of-privacy-report/.

- EPIC, Comments in re the Federal Trade Commission's Proposed Order & Settlement with Global Tel*Link (Dec. 2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-global-tellink/.

- Maria Villegas Bravo, DHS Disregards Internal Policies and Avoids Fourth Amendment Protections to Track Your Location, EPIC (Feb. 8, 2024), https://epic.org/dhs-disregards-internal-policies-and-avoids-fourth-amendment-protections-to-track-your-location/.

III. FinCEN should mandate data minimization and data deletion for third-party verifiers.

In response to Question 2 (b), (f),

To mitigate the potential for further financial surveillance, FinCEN should require banks to impose strong contractual data minimization and data deletion requirements, along with cybersecurity standards. Banks should enforce those contractual requirements through strong auditing procedures either by the bank or a vetted auditor.

In practice, data minimization requires the third-party verifier to collect or receive only the minimum information required to validate the SSN, without extraneous details like the type of bank account the consumer is applying for. The third-party verifier should delete any data from the bank when the transaction is completed and should not alter the verifier's file on the consumer. A third-party verifier should be in the business of facilitating the bank's SSN collection requirement, not accumulating a database of consumer's financial decisions that can be sold to advertisers or other buyers. FinCEN should also consider limiting third-party verifiers to not for profit services like the Social Security Administration's Social Security Number Verification Service, if such a service can handle the volume of requests from banks.

FinCEN can further protect consumer financial privacy by requiring banks to undertake strong, regularly conducted auditing of third-party verifiers. Auditing should cover all aspects of the verification transaction, from encrypted transmission to data retention or deletion.

IV. FinCEN should not encourage banks to rely on biometrics to validate identity, and should specifically avoid repeat, remote biometric verification.

In response to Question 6(b).

Biometrics are likely to become an increasingly weak form of identity verification. Machine learning and generative AI are quickly creating a world where spoofing face and voice biometrics will be all too easy. The presence of these technologies requires escalating countermeasures, like the rapid spread of facial liveness testing, that increase barriers for individuals to access services.

FinCEN should not take steps to promote biometrics for identity verification, the harms greatly outweigh the potential benefits.

Generative AI is already causing problems with fake images that are difficult to identify and voice imposters. Recently, a deepfake image of Pope Francis in a full-length Balenciaga puffy coat made news internationally for its realistic feel.[14] The celebrity deepfakes trend underscores a growing threat vector for digital identity fraud: using generative AI to fake identity. In 2021, a study found that common deepfake methods called generative adversarial networks (GANs) could trick advanced facial recognition systems. In the study, deepfakes were able to pass facial recognition systems 85 to 95 percent of the time.[15] Deepfakes continue to beat facial recognition systems to this day.[16] And deepfake attack vectors are growing as new video-manipulation techniques like face-swapping, facial reenactment, and facial manipulation come online.[17] As generative AI improves, facial recognition will become increasingly susceptible to attack, suggesting that using facial recognition as the basis for remote identity verification is not a sustainable practice.

Voice biometrics are subject to similar, even simpler attacks. Last year, journalist Joseph Cox was able to break into his own bank account using an AI-generated voiceprint.[18] Another journalist was able to fool an Australian government agency voiceprint system with generative AI earlier this

[14] *See e.g.* Kalley Huang, *Why Pope Francis Is the Star of A.I.-Generated Photos*, N.Y. Times (Apr. 8, 2023),
[15] *Id*.
[16] Milan Salco, Anton Firc, & Kamil Malinka*, Security Implications of Deepfakes in Face Authentication*, 39th ACM/SIGAPP Symposium on Applied Computing (2024), https://dl.acm.org/doi/pdf/10.1145/3605098.3635953.
[17] Anton Firc, Kamil Malinka, & Petr Hanaček, *Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors*, 9 Helyion 15090 (2023), https://www.cell.com/heliyon/pdf/S2405-8440(23)02297-1.pdf.
[18] Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.

year.[19] A paper testing the vulnerabilities of voice verification systems found that AI-generated voiceprints could successfully beat commercial voice verification systems 99 percent of the time given up to 6 tries per account.[20] Voiceprint verification has spread rapidly in the last few years, especially in the banking industry.[21] Lawsuits over non-consensual use of voiceprint verification have also multiplied.[22]

Using biometrics to validate identity poses similar threats to using SSNs because biometrics are immutable and often easily obtained. Just as a person cannot easily change their SSN, biometrics are based on a person's innate features and cannot be meaningfully altered. That means when a person's faceprint or voice is exposed to fraudsters, there is virtually no way for that individual to prevent biometric impersonations. Banks might reasonably rely on 1:1 on-device biometrics that function like unlocking an iPhone with your face. However, repeated remote biometric verification poses too many privacy risks and is likely to become unreliable. Banks should especially avoid using 1:many verification systems that check a face, fingerprint, or voice against a database of biometric prints. 1:many verification has increased error rates and poses substantially more privacy risks.

Conclusion

EPIC again urges FinCEN to 1) take all possible steps to reduce collection of SSNs online, 2) permit banks to obtain SSNs from third-party verifiers but not permit banks to collect other biographic information, 3) require strong data minimization and data deletion requirements for banks and third-

[19] Nick Evershed and Josh Taylor, *AI can fool voice recognition used to verify identity by Centrelink and Australian tax office*, The Guardian (Mar. 16, 2023), https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai.

[20] Andre Kassis & Urs Hengartner, *Breaking Security-Critical Voice Authentication*, 2023 IEEE Symposium on Security and Privacy 951 (2023), https://ieeexplore.ieee.org/abstract/document/10179374.

[21] Samantha Hawkins, *'Voiceprints' Roil Companies as Biometrics Litigation Skyrockets*, Bloomberg Law (May 18, 2022), https://news.bloomberglaw.com/privacy-and-data-security/voiceprints-roil-companies-as-biometrics-litigation-skyrockets; Jennifer A. Kingston, *Biometrics invade banking and retail*, Axios (Feb. 18, 2020), https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy.

[22] *Id*.

party verifiers, and 4) refrain from encouraging banks to use biometrics for identity verification. Please address any questions to EPIC Fellow Suzanne Bernstein at bernstein@epic.org.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Counsel

Suzanne Bernstein
Suzanne Bernstein
EPIC Fellow