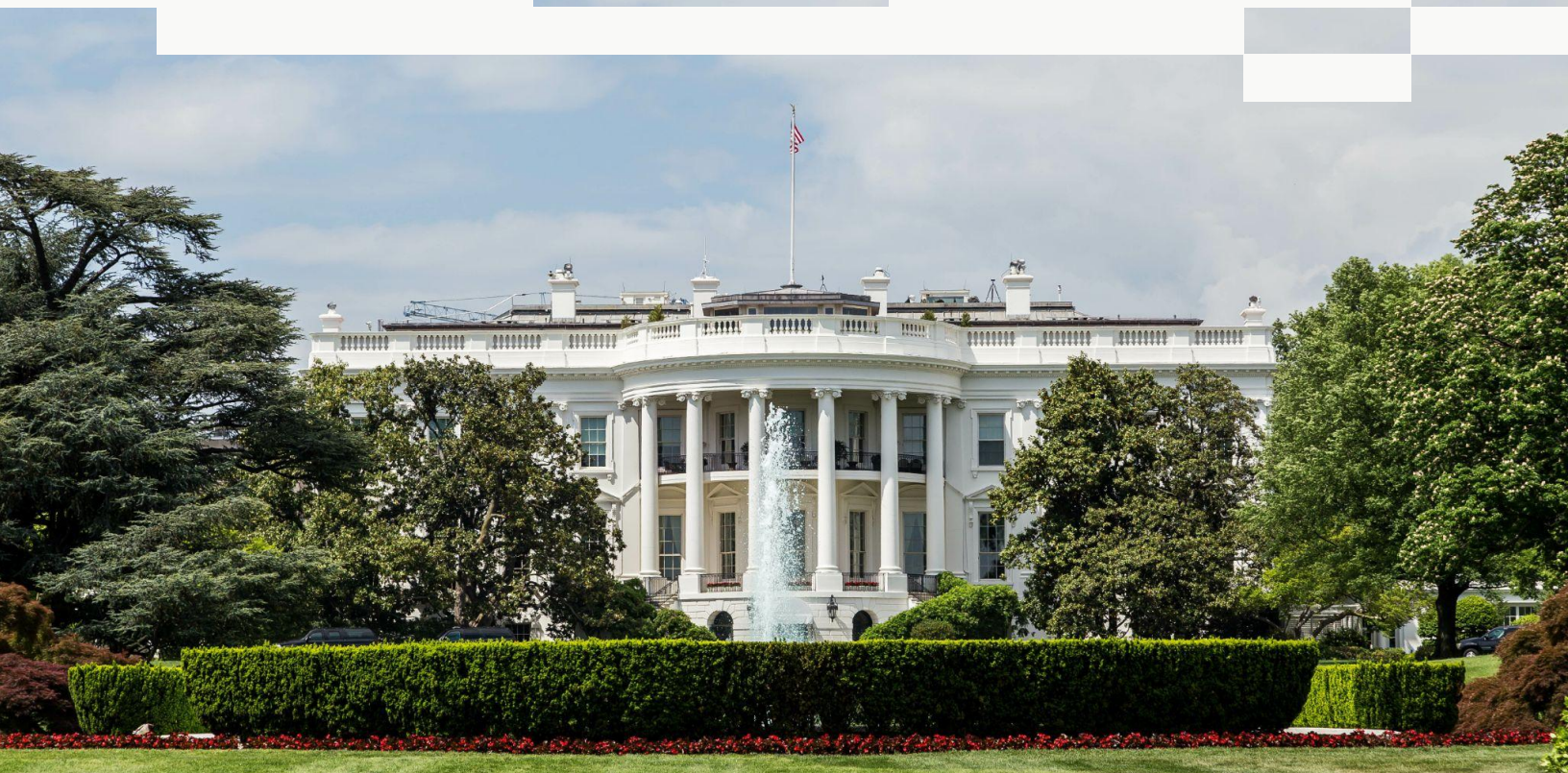
Proof[SM]

A Blueprint for the Incoming Administration: How to Save Americans $1 Trillion Per Year

December 2024

Pat Kinsel, CEO & Founder, Proof



America has a $1 trillion fraud problem. The tools to solve it are readily available. The following blueprint is a guide to the incoming administration for creating a government that works better for the people and is free from fraud.

Commit to Making the Federal Government More Efficient for the American People:

The federal government manages over 9,000 unique forms, processing more than 100 billion forms each year, costing the government over $38 billion annually in direct processing costs. This burden extends far beyond the government, imposing an additional strain on the public that results in 10 billion hours of time and over $100 billion annually complying with government paperwork.[1]

To make the government more efficient and simplify processes for all Americans, the Trump Administration should issue an Executive Order addressing the government's overreliance on paper. The order should direct the Office of Management and Budget (OMB) to audit the implementation of the 21st Century Integrated Digital Experience Act[2], which President Trump signed in December 2018. Guidance issued by OMB in 2023[3] requires agencies to digitize forms and accept electronic signatures. The administration should accelerate implementation and ensure that every agency is on track to remove existing outdated wet ink signature requirements by June 30, 2025, the 25th anniversary of the Electronic Signatures in Global and National Commerce Act.

Additionally, the administration should build upon initiatives started in the first Trump Administration, particularly the U.S. Department of the Treasury's efforts[4] to expand remote online notarization and fully digitize outstanding paper-dependent processes.

Paper-based processes pose significant risks beyond inefficiency and high costs, making them a prime target for fraudsters, especially in contrast to increasingly secure digital processes. The vulnerabilities of paper-based systems are stark: They are inherently susceptible to impersonation and forgery, lacking the robust protections available through digital channels. A striking example is America's use of paper checks. Although check use remains on a steady decline, representing a little over 30% of all payments, they account for 66% of payment fraud[5].

The administration's actions to move agencies away from paper to digital solutions will position the United States as a global leader in innovation, streamline operations, reduce bureaucratic delays, and make essential services more accessible to all Americans. Additionally, digital alternatives will eliminate the "time tax" that traditionally burdens Americans, ensuring

[1] U.S. Chamber of Commerce, Technology Engagement Center, "Government Digitization: Transforming Government to Better Serve Americans," October 17, 2022
[2] 21st Century Integrated Digital Experience Act, 44 U.S.C. § 3501 (2018)
[3] Office of Management and Budget, M-23-22, "Delivering a Digital-First Public Experience," September 22, 2023
[4] U.S. Department of the Treasury, "A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation," July 2018
[5] Association of Fraud Professionals, "Digital Payments Survey Report," 2022; Association of Fraud Professionals, "Payments Fraud and Control Report," 2022

faster, more accurate delivery of critical government services.

Establish Identity-Centric Policies to Improve Efficiency and Eliminate Fraud:

A key driver of waste across the federal government stems from significant levels of fraud throughout government programs. Initial estimates indicate that the government lost as much as $400 billion[6] to fraud delivering COVID-19 pandemic assistance programs, but more recent reports suggest that the actual number is closer to $1 trillion.[7] Even without pandemic-related assistance, the government loses hundreds of billions[8] in government dollars every year to fraud. Eliminating annual losses would reduce the federal government's annual deficit by as much as 28%[9].

To combat these systematic issues, the Trump Administration should direct agencies towards an identity-centric model for accessing government services.

Identity-centric policies are grounded in a commonsense principle that the individual who completes, signs, and submits something to the government is really who they say they are.

In conjunction with efforts to digitize the government, the administration should require all documents submitted electronically to be digitally signed with a tamper-evident certificate tied to a verified identity.

It is not enough to simply require Americans to verify their identity when they interact with government agencies or request government services. Proof of their identity must travel with the documents and records they submit so systems and individuals downstream have the certainty required to make immediate and automated decisions.

In other words, what is the value of requiring identity verification when using a tax preparation platform if the Internal Revenue Service (IRS) cannot validate the evidence that was used to verify the individual who authorized and submitted the tax return?

Done properly, automated systems and individuals should have instant proof of authenticity and trustworthiness when reviewing something via a visual indicator. Just as a padlock symbol on a website instantly communicates secure encryption, or a green checkmark in a digital document indicates its integrity.

What is most important is that nothing needs to be invented to implement these improvements; the solutions are shovel-ready. The private sector can immediately provide the government with the tools required. Existing federal policies and open standards are already in place to govern identity verification (NIST IAL2[10]),

[6] Associated Press, "The Great Grift: How billions in COVID-19 relief aid was stolen or wasted," June 12, 2023
[7] Rolling Stone, "The Trillion-Dollar Grift: Inside the Greatest Scam of All Time," July 9, 2023
[8] U.S. Government Accountability Office, "Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments," April 16, 2024
[9] United States Department of the Treasury, Fiscal Data, "U.S. Deficit Compared to Revenue and Spending, FY 2024"

[10] National Institute of Standards and Technology, "NIST Special Publication 800-63A," June 2017

digital certificate use (e.g., AATL[11]), and authentication (NIST AAL2[12]). Importantly, digital certificates create a privacy-preserving approach to identity verification that supports data minimization efforts. Systems are designed to the latest data and cybersecurity standards and can even be future-proofed with quantum-resistant cryptography.

Furthermore, agencies can leverage existing solutions to set up automated submission gateways to enable seamless web-based execution and submission. These solutions automate verifying document accuracy, confirming document integrity, validating digital signatures and certificates, and routing documents for manual review and approval when necessary.

Perhaps the most persuasive evidence supporting the need for identity-centric policies is the rampant fraud experienced throughout the Small Business Administration's (SBA) two pandemic assistance loan programs. The SBA's two programs are estimated to have lost over $200 billion to fraud. At least $70 billion of which came from applicants with foreign IP addresses, including individuals with expected involvement in international criminal organizations[13], despite the program's availability to only businesses located in the U.S. or its territories. The SBA requires that lenders use a NIST IAL2-based electronic signature solution. However, evidence suggests this policy is not being enforced, and SBA applicants are still submitting forms without proper identity verification. In response, the administration should examine all existing agency identity and security policies to ensure that government agencies rigorously enforce existing anti-fraud standards to eliminate waste and protect taxpayer resources.

To achieve widespread success, the administration should ensure these policies are accessible to all Americans. Increased accessibility will not only improve the citizen experience for all but will ensure that the government's interactions with every constituent are secure. Central to this is establishing clear policies that enable humans to intervene to assist applicants when necessary. Various factors, such as limited familiarity with digital tools, user error, or system error, can make it difficult for some individuals to complete automated identity-proofing processes. NIST's latest IAL2 guidance[14] addresses these challenges and sets clear policies for the role humans serve as trusted agents that can assist applicants that failover, ensuring broad availability.

An identity-centric model for government services will enhance government efficiency by automating submissions and approvals, reducing manual intervention, and minimizing the potential for human error. In turn, these actions will eliminate the waste stemming from fraudulent applications or losses due to misappropriation when funds are sent to the wrong person.

[11] Adobe, Adobe Approved Trust List, last updated on May 24, 2023; ITU-T X.509: Public-Key and Attribute Certificate Framework; ISO/IEC 9594 Open Systems Interconnections; IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL); RSA Public Key Cryptography Standards (PKCS); NIST FIPS 186 Digital Signature Standard

[12] NIST, "NIST Special Publication 800-63B," June 2017

[13] U.S. Small Business Administration, Office of Inspector General, "COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape," June 27, 2023

[14] NIST, "NIST Special Publication NIST SP 800-63A-4 2pd," August 2024

Secure Official Communication and Records from Fraud and Misinformation:

The rapid advancement of generative AI, deepfakes, and forgery has eroded what is left of the public's trust in institutions.

To regain this trust, the Trump Administration should adopt industry-leading standards for content authenticity and watermarking and commit to issuing all communications from the White House with verifiable metadata indicating the source and provenance of all content. Again, existing open standards can guide the administration's actions. The Coalition for Content Provenance and Authenticity[15] (C2PA), for example, has been embraced by Adobe, Amazon, Microsoft, and others as the solution to generative AI-enabled fraud, forgery, and deepfakes. Any content produced in accordance with C2PA standards will be cryptographically signed and verifiable across the majority of internet services and business applications.

Correspondingly, the administration should take action to restore trust across all federal government communications, records, and forms, whether it be a permit or authorization to drill or build, or an agency alert in time of a national emergency. Americans need certainty in the content the government publishes. To that end, the administration should require all federal agencies to embed verifiable metadata in all content to give receiving parties trust and confidence and prevent manipulation. Existing policies already required agencies to transition records and publications to an electronic format by June 30, 2024,[16] and some metadata requirements[17] are already in place. Conforming to more modern industry standards like C2PA will both improve the verifiability of records and also streamline agency compliance with existing rules.

---

[15] Coalition for Content Provenance and Authenticity

[16] Office of Management and Budget, M-23-07, "Update to Transition to Electronic Records," December 23, 2022

[17] U.S. National Archives and Records Administration, "Metadata Requirements for Permanent Electronic Records"

Practical Examples in Government:
Identity-centric policies and secure government communications will reduce forgery and streamline processing times across the government and private sectors.

Improving the IRS Form 1040, the U.S. Individual Income Tax Return: *Upon downloading Form 1040 from irs.gov, the file will contain cryptographically embedded metadata proving it was generated by an official government source, and information about where and when it was obtained. As a taxpayer completes the form, information about what is changed can be clearly displayed in a corresponding audit log. When a taxpayer is ready to sign, they will do so digitally with a certificate tied to their verified identity. When the completed Form 1040 is returned to the IRS, systems can automatically ingest and read the metadata contained within the file, verifying that the original document was obtained from the IRS, was not improperly manipulated, and was executed and signed by a verified taxpayer.*	**Improving the Form W-2, Wage and Tax Statement:** *When the Social Security Administration processes W-2 forms, the file will contain cryptographically embedded metadata verifying the legitimacy of the submitting business, giving downstream participants verifiable proof of their origins. When W-2 information is passed to the IRS during tax season, the metadata will enable automated verification. The metadata will also help to secure financial transactions by providing banks and lending institutions a means to verify that income statements were produced by legitimate employers and the form was not manipulated.*

Embrace Innovative American Technologies Throughout the Public and Private Sector:
The private sector is grappling with a rising tide of fraud that rivals the challenges faced by the government. The Financial Crimes Enforcement Network[18] (FinCEN) reports alarming trends, with financial services suffering $80 billion in annual losses from sophisticated fraud schemes, including falsified records, forged signatures, and identity theft.

Recent analysis[19] highlights a dramatic escalation in fraudulent attacks in recent years. Retail and commercial banks, along with wealth management institutions, have experienced over 50% more incidents while lending institutions—including auto lenders and mortgage companies—have seen an even more startling increase of over 150% in successful attacks.

[18] U.S. Financial Crimes Enforcement Network, Financial Trend Analysis, "Identity-Related Suspicious Activity: 2021 Threats and Trends," January 2024

[19] LexisNexis® Risk Solutions, "2023 LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending Report," April 24, 2024, *Data Note: Calculated based on the average monthly fraudulent transactions reported by LexisNexis in 2023.*

The threat is rapidly evolving with technological advances. Deloitte[20] predicts that generative AI will likely cause banks and their customers to incur fraud losses of up to $40 billion annually by 2027. A recent TransUnion[21] study underscores the severity, revealing that industries lost nearly 7% of their revenue—approximately $112 billion—to fraud in the past year.

These staggering figures make one thing clear: the private sector is hemorrhaging hundreds of billions of dollars annually to fraudulent activities.

Much of this fraud can be stopped by improving information sharing across federal agencies and reducing the limitations on what information can be shared between private companies.

Efforts by U.S. financial regulators to combat money laundering and terrorist financing are crucial, but the current approach warrants reassessment. Given the escalating complexity and frequency of fraud in the U.S., the administration should develop more proactive strategies to protect Americans from fraud. The administration should determine if existing regulatory frameworks, including the Suspicious Activity Reporting (SAR) requirements, are adequately designed to address today's challenges.

Existing policies for addressing criminal activity are fundamentally reactive in nature. Most financial institutions submit SARs only after transactions have been processed.

While these reports are helpful to investigations and law enforcement, they are ineffective for fraud prevention. This approach not only fails to stop criminal activity in real time but also generates massive databases of personal information with minimal practical utility. Instead, the administration should introduce a modern framework inspired by America's leading payment networks to create a privacy-preserving approach to fraud detection and prevention.

Drawing inspiration from credit card networks, where private companies collaboratively improve security by sharing fraud indicators, a network within financial services based on tokenized identities could revolutionize fraud prevention. For instance, if a fraudster using personal information obtained from the dark web attempts to secure a loan at Bank A and is rejected due to suspected fraud, the network could immediately alert other participating banks. By sharing this real-time fraud intelligence, subsequent loan applications could be automatically declined across multiple institutions, disrupting the fraudster's ability to exploit the entire network.
Privacy-preserving technologies exist and can be deployed with low friction, enabling fraud detection without exposing sensitive personal information.

Defending against increasingly sophisticated fraud requires that public and private sectors are permitted to deploy equally advanced countermeasures. To ensure this, the administration should establish, where necessary, regulatory sandboxes to allow critical industries to embrace new technologies designed to

[20] Deloitte Center for Financial Services, "GenerativeAI is expected to magnify the risk of deepfakes and other fraud in banking," May 29, 2024
[21] Transunion, "H2 2024 Update: State of Omnichannel Fraud Report," October 16, 2024

respond to modern fraud threats. White House and agency-level policies should promote the expanded use of biometric-based identity verification tools and ensure the continued availability of advanced algorithms that provide real-time data on suspected fraudulent activity. Furthermore, the administration should examine all existing agency identity and security policies to ensure digital identity credentials, such as digital certificates based on public key infrastructure (PKI)[22] technology, can be used to authenticate and secure identities in online environments.

Recently, the peer-to-peer payment service Zelle[23] was made to update its consumer reimbursement policies after failing to meet a "standard of care" that is yet to be defined by the government. Similarly, Citibank[24] is facing a lawsuit for allegedly failing to provide adequate protection against unauthorized account takeovers. Without agency-level directives that enable information sharing and the use of innovative technologies, these institutions' ability to respond to growing fraud threats will be limited. The administration has the opportunity to provide clear regulatory guidance, enabling the private sector to better protect consumers from fraud.

Conclusion:

As fraud threats continue to evolve at an unprecedented pace, existing challenges confronting both the federal government and private enterprises demand immediate and comprehensive action. Making robust technological and strategic improvements to our institutional infrastructure is critical to enhancing government efficiency, protecting taxpayer interests, and maintaining national and economic security. Since our founding, Proof has remained a partner and trusted resource to all levels of government, advancing policies that prioritize consumer safety, accessibility, and the future of digital commerce. This blueprint provides the incoming administration with a plan to save taxpayers billions and strengthen the integrity of the nation. We look forward to working with our partners in the federal government to facilitate it.

---

[22] *See 11*
[23] Reuters, "Payments app Zelle begins refunds for imposter scams after Washington pressure," November 13, 2023
[24] Reuters, "Citibank sued by New York over alleged failure to reimburse fraud victims," January 30, 2024

About Proof:
Proof is the trusted platform for the most important agreements that businesses and consumers sign. More than 7,000 businesses trust Proof to collect all types of documents - everything from online notarization to identity-assured eSignatures. The platform combines strong identity verification with built-in fraud prevention to ensure signatures are harder to forge. Proof operates the Notarize Network, the largest on-demand network of trusted notaries that are available 24/7 to perform a notarization or check a person's identity. For more information, visit: www.proof.com.

Contact:
James Fulgenzi, james.fulgenzi@proof.com