Office of Inspector General | United States Postal Service

RISC Report

The Role of the Postal Service in Identity Verification

Report Number RISC-WP-22-006 | May 11, 2022

BACK *to* COVER

Table of Contents

Executive Summary

When an individual applies for a benefit or service at a government office or through an online account, the agency must verify their identity to ensure they are who they claim to be. To do so, the agency verifies the applicant's identity credentials or attributes, such as a name, address, Social Security Number, or biometric features. Verifying the identity credentials that individuals provide online — or digital identity — has been a growing challenge for government agencies. Fraudsters have increasingly used fake or stolen identities to claim government benefits. During the COVID-19 pandemic, the emergency disbursement of trillions of dollars in government relief funds increased the incentive for fraudsters to target government programs, leading to unprecedented levels of identity fraud and improper benefit payments.

To prevent identity fraud and encourage more secure identity proofing, the federal government has launched several measures. The American Rescue Plan Act (ARPA) funds agencies' initiatives aimed at strengthening their identity verification systems and ensuring equitable verification for vulnerable populations. In addition, many agencies have partnered with private sector providers to implement more secure and advanced remote verification methods and technologies, such as facial recognition software, biometrics collection devices, and artificial intelligence.

However, each verification method has different strengths and limitations, and the most stringent verification standards still involve in-person proofing (IPP) — where a user physically presents their identification documents for review by an authorized representative attesting to their accuracy and authenticity. IPP is currently available to USPS customers at 17,000 retail locations for services that require identity verification, such as renting a PO Box or enrolling in Informed Delivery. More recently, USPS has piloted two more complex forms of in-person verification services involving the collection of biometrics, in partnership with the General Services Administration (GSA) and the FBI, at selected postal retail locations.

The U.S. Postal Service Office of Inspector General (OIG) conducted research to identify opportunities for the Postal Service to support the federal government's efforts to promote secure identities by leveraging some of its major assets. This includes a vast retail network, databases of the nation's addresses, and experience with identity verification. As government and commercial actors implement new identity verification strategies and partnerships, a window of opportunity is currently open for the Postal Service to respond to their needs for more secure verification and to better serve all citizens.

Based on an analysis of the identity verification challenges government agencies currently face and interviews with government agencies and private sector providers, we identified three potential roles for the Postal Service in identity verification: as a provider of IPP, a validator of individual's identity attributes (personal identifiers such as names and addresses), and a provider of postal digital identities. Government agencies and private identity verification companies we interviewed saw a higher public service and commercial value in the Postal Service's implementing the first two concepts.

First, USPS could gradually extend current IPP services to the customers and employees of other federal and state agencies nationwide. The service would increase convenience for citizens completing transactions that need high levels of identity assurance and provide a fallback option for government customers who have failed remote identification verification or prefer in-person interaction. It would also help vulnerable citizens with no or limited credit history, or without access to broadband Internet, verify their identity. Finally, the Postal Service could offer IPP in coordination with organizations involved in assisting victims of identity fraud to help these individuals reestablish their identity credentials and regain access to their government accounts.

Second, in addition to IPP, the Postal Service could provide name/address validation services. Subject to user's prior consent, the verification service would calculate the level of confidence that this person lives at the address provided. The service would help increase the confidence of government agencies and their verification partners that a user creating an online account is who they claim to be.

Finally, the Postal Service could also explore whether and how its 47 million Informed Delivery subscribers could, in the long term, use their verified postal credentials to prove their identity to securely create and access other government accounts.

While estimating the demand for identity verification services was outside the scope of this paper, the high level of identity fraud and the federal government's focus on closing identity verification gaps demonstrate the potential value of these services to government, citizens, and the private sector. However, since the Postal Service does not receive appropriations, it would have to rely on alternative funding sources to support the expansion of its verification services to the public. These sources could include a combination of government funding, interagency reimbursable work agreements, and service fees. Finally, the recent passing of the Postal Service Reform Act of 2022 expands the Postal Service's ability to provide nonpostal services, such as identity verification, to all levels of government, not just federal agencies. Further legislative action allowing the provision of identity services to private sector businesses would allow the Postal Service to fully maximize the commercial and social value of these public interest services.

Observations

Introduction

When an individual applies for a benefit or service at a government office or through an online account, the agency must verify the individual's identity (ID).[1] To vouch for their unique identity, the user provides a set of identity credentials or attributes, such as a name, address, Social Security Number (SSN), or biometric features.

The government services Americans rely upon are being increasingly provided online. This makes the need for a digital ID to access them just as vital as our physical identity. Akin to the verification of users' physical identities, the verification of digital IDs — also called ID proofing — involves three key steps:[2]

1. Resolution: the user presents identity attributes to distinguish their identity ("Is this the right John Smith?");
2. Validation: the presented identity attributes are authenticated and determined to be legitimate ("Are John Smith's documents valid?"); and
3. Verification: the validated attributes are determined to belong to the user who presented the evidence ("Is the applicant really John Smith?").

Verifying the identity of users opening an account on a government site helps prevent bad actors from using stolen identity to commit fraud. However, the COVID-19 pandemic exposed underlying vulnerabilities with identity verification systems within many government agencies. The temporary closure of many consumer-facing government offices forced agencies to rapidly transition to fully online processes. In addition, the emergency disbursement of large amounts of government funds increased the incentive for fraudsters to target government programs. These factors resulted in unprecedented levels of identity fraud and improper payments in government programs.

The pandemic has highlighted the need for government agencies to implement stricter ID verification systems to respond to these challenges. As such, federal and state governments have been taking steps to combat increased attempts to steal and forge digital IDs to fraudulently claim government benefits.

In this fast-evolving environment, the U.S. Postal Service Office of Inspector General (OIG) examined the current landscape of identity verification in the United States. Our objective was to better understand potential opportunities for the Postal Service to contribute to government efforts to create and implement more secure identity verification systems. We first discuss challenges and trends in ID verification and the U.S. government's responses to ID fraud. Then we discuss several concepts illustrating potential roles for the Postal Service in ID verification. See Appendix A for more details on this project's objectives, scope, and methodology.

The Challenge of ID Fraud for Government

While identity fraud has been a growing challenge over the last two decades, the pandemic exacerbated this issue and revealed the underlying vulnerabilities of government identity verification systems.

ID Theft and Fraud Have Expanded Over the Past 15 Years

ID theft — the stealing of personal identifying information — is not a new phenomenon. The Identity Theft and Assumption Deterrence Act of 1998 made ID theft a federal crime. Fraudsters use a variety of techniques to access passwords and personally identifiable information (PII). For example, people inadvertently share personal information on social media or fall victim to phishing attacks by responding to fraudulent emails. Large-scale data breaches have lowered barriers to fraudulently access PII. In particular, the 2017 Equifax data breach exposed the private records of 148 million Americans. According to the Identity Threat Resource Center (ITRC), the annual number of reported data breaches in the United States has increased from 785 cases in 2015 to 1,862 in 2021.[3] The Aite Group has estimated that 47 percent of Americans experienced financial identity theft in 2020.[4]

[1] For the purposes of this paper, we will use identity and ID interchangeably.
[2] For the purposes of this paper, we will use ID proofing and ID verification interchangeably.
[3] Identity Theft Resource Center, 2021 In Review – *Data Breach Annual Report*, January 2022, accessed at https://notified.idtheftcenter.org/s/2021-data-breach-report.
[4] Financial identity theft is the compromise of an existing financial account or the creation of new financial accounts by an unwanted third party. Aite Group, "U.S. Identity Theft: The Stark Reality," March 9, 2021, https://aite-novarica.com/report/us-identity-theft-stark-reality.

Easy access to passwords and other personal information allows fraudsters to commit ID fraud, to include using stolen identities to create illegitimate accounts and inappropriately apply for government benefits. Bad actors can also redirect payments from legitimate beneficiary accounts to accomplices by changing bank account information (known as redirection fraud). In addition to stealing existing identities, perpetrators can create synthetic identities. Creating a synthetic identity consists of supplementing an individual's real personal information with made-up data, such as addresses. Using this information, fraudsters may, for example, obtain credit and debit cards, which they can then use to apply for government loans. As a result of these trends, paper-based government-issued credentials — such as an SSN — are no longer sufficient for citizens to prove who they are in a digital environment. In fact, in 2021, a valid SSN could be purchased for only $2 in criminal online marketplaces.[5]

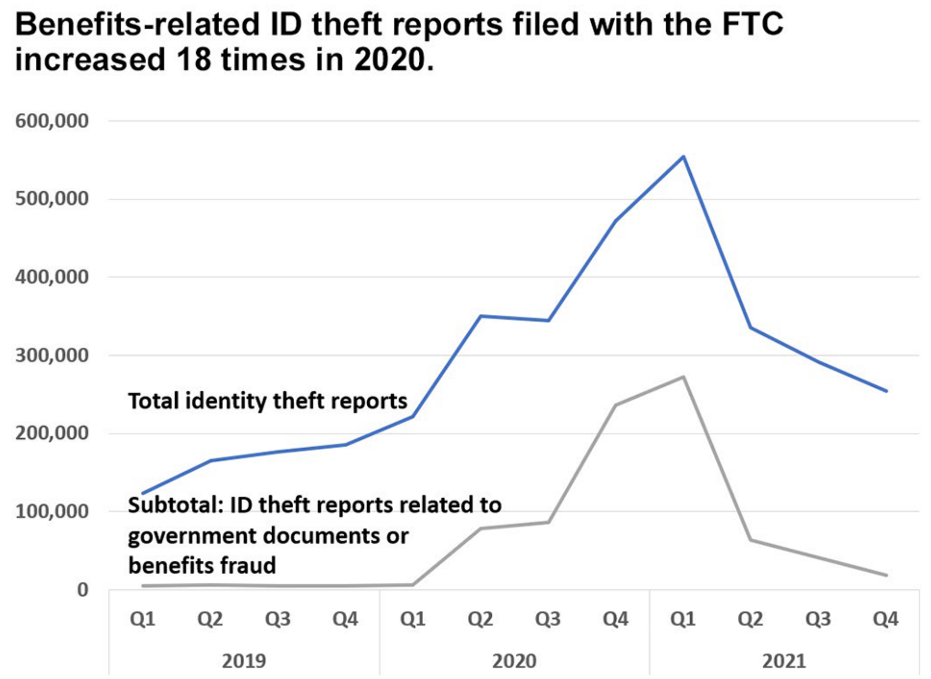
ID Theft and Fraud Reached Unprecedented Levels during the Pandemic

The emergency disbursement of trillions of dollars in government relief funds increased the incentive for fraudsters to target government programs, leading to unprecedented levels of identity fraud and improper payments in government programs.

Growth in ID Theft Reports

The Federal Trade Commission (FTC) received 1.4 million ID theft reports in 2020 and again in 2021, up 113 percent from 650,000 in 2019. Much of this increase was driven by the significant growth in the number of complaints of stolen identities being misused to apply for government benefits. At about 400,000 in 2020, this number was 18 times higher than the year before (Figure 1).

Figure 1: Trends in ID Theft Reports Calendar Year 2019 – 2021



Source: FTC Consumer Sentinel Network.

After peaking at the end of 2020, ID theft reports related to government benefits dramatically declined starting in the second quarter of 2021. The decline coincided with the end of funding for the main pandemic relief programs and expansions, as well as with rising government oversight and program integrity efforts.[6]

Increased Transactions Volume Stretched Agencies' Systems

The volume of online applications for government pandemic relief funds stretched agency systems and staff. The pressure to quickly provide temporary benefits to millions of recipients led many agencies to loosen internal controls and access

[5] Zachary Ignoffo, "Dark Web Price Index 2021," Privacyaffairs.com, February 3, 2022, https://www.privacyaffairs.com/dark-web-price-index-2021/.
[6] Federal unemployment benefit programs under the CARES Act ended on September 4, 2021. U.S. Federal Trade Commission, "Fraud and ID Theft Maps: ID Theft by State," FTC Consumer Sentinel Network, February 22, 2022, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/IDTheftbyState.

requirements. For example, some agencies relaxed individual reviews and verifications and ignored systems flags.[7]

As of February 2021, over half the states were still relying on outdated IT equipment that limited their ability to detect and prevent fast-growing fraudulent claims.[8] The combination of inadequate verification methods, outdated IT systems, and low staffing levels left agencies ill-prepared to effectively manage the surge in applications and detect fraudulent activities.

Many Improper Payments Were Caused by ID Fraud

The Pandemic Response Accountability Committee (PRAC) noted that many improper government payments during the pandemic resulted from ID verification issues and insufficient internal controls of claimants' self-declarations.[9] According to the Office of Management and Budget (OMB), the government-wide improper payment rate rose from 5.6 percent to 7.2 percent between fiscal year FY 2020 and FY 2021.[10]

For unemployment (UI) benefits specifically, the percentage of improper payments was even higher: 18.7 percent from July 2020 to June 2021. For example, the Department of Labor (DOL) OIG identified $17 billion in potentially fraudulent UI benefits. The questionable payments were made to individuals with SSNs filed in multiple states, claimants with SSNs from deceased persons and federal inmates, and those with suspicious email accounts.[11]

In total, OMB estimated that $281.4 billion in government (pandemic and non-pandemic) benefits were paid improperly in FY 2021, with a significant portion attributable to ID fraud.[12]

Secure ID Verification Solutions Help Prevent Fraud

To support government digital identity verification and fraud prevention needs, credit reporting agencies (CRAs), ID verification companies, and other technology providers have developed a variety of remote identity verification methods and technologies. The Postal Service has taken a different strategic approach that leveraged its retail network and positioned itself mostly as a provider of in-person verification.

Identity verification methods vary in their ability to prevent fraud. Agencies generally select the most appropriate combination of verification methods based on resource availability and level of risk associated with the information they handle. The higher the risk and potential impacts of fraud, such as financial losses, the more stringent the identity assurance level (IAL) and the verification methods must be. The National Institute of Standards and Technology (NIST) has developed guidelines that describe the three IALs and outline the verification methods a government agency may use to achieve them.[13] Based on their risk profile, many customers' government accounts generally require medium levels of assurance (IAL2).[14] Unlike NIST IAL1, where identity attributes are self-asserted, IAL2 and 3 levels necessitate the use of remote or in-person identity proofing techniques to detect fraudulent identities. While the most rigorous IAL3 requirements necessitate

NIST IAL1, 2, and 3 levels of assurance prescribe requirements for validating and verifying identities. The most rigorous level, IAL3, requires in-person verification and the use of biometrics.

[7] SBA Office of Inspector General, *Inspection of Small Business Administration's Initial Disaster Assistance Response to the Coronavirus Pandemic*, Report No. 21-02, October 28, 2020, https://www.sba.gov/document/report-21-02-inspection-small-business-administrations-initial-disaster-assistance-response-coronavirus-pandemic, p.24, and PRAC, *Key Insights: State Pandemic Unemployment Insurance Programs.*

[8] Pandemic Response Accountability Committee (PRAC), *Key Insights: State Pandemic Unemployment Insurance Programs*, December 16, 2021, https://www.pandemicoversight.gov/media/file/state-unemployment-insurance-capping-report.

[9] PRAC is a committee of the Council of the Inspectors General on Integrity and Efficiency.

[10] OMB, "Updated Data on Improper Payments", December 30, 2021," https://www.whitehouse.gov/omb/briefing-room/2021/12/30/updated-data-on-improper-payments/.

[11] Department of Labor OIG, "DOL-OIG Oversight of the Unemployment Insurance Program," https://www.oig.dol.gov/doloiguioversightwork.htm.

[12] OMB, "2021 Annual Improper Payments Dataset," version dated March 14, 2022, https://www.cfo.gov/payment-accuracy/FY2021%20Payment%20Accuracy%20Dataset_3_14_2022.xlsx.

[13] NIST is a unit of the U.S. Department of Commerce that develops measurement solutions and technological standards.

[14] For a description of the three identity assurance levels (IAL 1, 2 and 3), as defined by NIST, see Appendix B, and A. Grassi, et al., *NIST Special Publication: Digital Identity Guidelines*, SP 800-63-3, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

in-person verification and the use of biometrics, such as fingerprints, both are optional at the IAL2 level.

ID Verification Methods and Technologies

The ID verification solution market is constantly evolving thanks to the introduction of new and more sophisticated technologies and methods, which either complement or substitute existing ones. Each verification method has different strengths and limitations. Using a combination of two or more of these methods can help increase their effectiveness in preventing ID fraud.

Knowledge-Based Verification

To perform remote knowledge-based verification (KBV), individuals are asked a series of multiple-choice questions based upon their life history. CRAs utilize information compiled from consumer credit files to generate the questions. However, an increase in data breaches has led to more questions about the ability of KBV systems to prevent ID fraud. An attacker may fraudulently obtain and use an individual's personal information to successfully answer the knowledge-based questions.

For this reason, many government agencies are moving away from KBV for identity verification purposes.[15] In 2017, NIST recommended that KBV no longer be used to verify identities for sensitive applications such as user's accounts with federal agencies. In 2019, OMB issued guidance for agencies to implement the NIST standards.[16] However, at the start of the COVID-19 pandemic, not all federal agencies had abandoned KBV systems.[17] For example, State Workforce Agencies (SWAs) were still using this method for traditional UI benefits and for the temporary UI expansion programs.[18]

ID theft risk is not the only limitation of KBV. Having no credit history or credit report with any of the three national CRAs means some people may not be able to get verified through KBV systems and other validation methods that rely on credit-based information. A study from the Consumer Financial Protection Bureau shows one in ten adult Americans (26 million people) are "credit invisible."[19]

Attribute Validation

Identities are comprised of attributes — including name, address, date of birth, and phone number — among other personal information. Attribute validation involves conducting crossmatches of individuals' submitted information with available databases, such as phone carriers' customer databases or a state's department of motor vehicles database. The validation may involve sending a code to a remote applicant's phone or by mail. Attribute validation, however, may not fully eliminate ID theft risks. For example, attackers may try to manipulate or "spoof" phone numbers that redirect phone calls and confirmation codes.

Remote Document Verification

Remote document verification starts with scanning and sending a copy of a driver's license, state ID, or passport, and the use of authoritative databases of document types and artificial intelligence technology (AI) to verify authenticity of the document. However, scanning and sending a copy of an identity document does not explicitly prove that the applicant is the document holder. To add another layer of verification for remote document verification, the applicant takes a live selfie that is compared with the picture on the previously uploaded ID document. This comparison involves the use of machine learning and facial recognition technology to conduct a liveness check and confirm that the two pictures match.[20]

[15] Agencies are also moving away from security questions as a method for authenticating users when they access their accounts to embrace multi-factor authentication (MFA). This means that in addition to a password, customers select additional authentication methods, such as a one-time password, face or touch unlock on a smartphone, or security keys to securely access their account. See for example, "Authentication Options," Login.gov, https://www.login.gov/help/get-started/authentication-options/.

[16] Office of Management and Budget (OMB), "Memorandum M-19-17," May 21, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf. At about the same time, GAO also recommended discontinuation of KBV. GAO, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, GAO-19-288, https://www.gao.gov/assets/700/699581.pdf, p.30.

[17] For example, the U.S. Small Business Administration (SBA) relied on KBV from applicants' credit history to verify identities for the COVID-19 Economic Injury Disaster Loans program. U.S. Small Business Administration (SBA), *COVID EIDL Portal Instructions*, September 8, 2021, https://www.sba.gov/sites/default/files/2021-09/COVID-EIDL-Portal-Instructions-090821-508.pdf, p.7.

[18] U.S. Department of Labor Employment & Training Administration, *Advisory: Unemployment Insurance Program Letter No. 16-21*, April 13, 2021, https://wdr.doleta.gov/directives/corr_doc.cfm?docn=9141, p.5.

[19] CFPB Office of Research, *Data Point: Credit Invisibles*, Consumer Financial Protection Bureau, May 2015, https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf, p.6.

[20] Liveness checks are used to confirm that the submitted selfie photo is from a live person and not a spoofing, impersonation, or presentation attack.

A shortcoming of this method is biometric bias.[21] A comprehensive academic review of studies conducted on this bias found that "current algorithms tend to exhibit some degree of bias with respect to certain demographic groups."[22] A 2019 NIST study reached the same conclusion. False positive rates — incorrectly matching two different images — could be ten to one hundred times higher for Asian and African American faces than for Caucasian faces. False positive and false negative rates — a failure to match two images of the same person — were also higher for women and younger people.[23]

Predictive Identity Validation

Several companies have developed predictive identity validation models combining a variety of personal identifiers to verify if all these identities are linked together, or if there are inconsistencies that may indicate potential fraud. For example, Experian's identity verification (IDV) tool computes ID theft scores and associated cause codes, which allows a company or agency to assess whether an online claim may be potentially fraudulent.[24] Although predictive modeling can flag suspicious accounts, this method alone cannot verify that an applicant is who they claim to be.

Shareable Digital IDs

Shareable IDs are not an ID verification method, but rather a way for users to avoid creating and verifying a new digital ID each time they create an account on or access a new website. Users create a verified digital ID once and reuse it to securely log into all the websites that accept that verified ID. Shareable, or portable, identities could speed up the adoption of new, more secure ID verification strategies by government agencies. A notable example is the GSA Login.gov single sign-on service. Users can create one account to access the websites of all participating federal agencies. Another example is the mobile driver's license (mDL) tested by several states. Consumers use an app (called a digital wallet) to store credentials issued by a government agency or an academic institution. The consumer will be able to use the wallet to confirm elements of their identity, prove eligibility to a service, or complete a transaction. However, this service would not be available to people without a smartphone or access to the Internet.[25]

On-site and Remote In-person Proofing

On-site in-person proofing (IPP) involves a trained professional making a direct physical comparison of an individual's physical features with a physical credential, such as a driver's license or passport. The clerk also manually inspects and authenticates the physical identification document. IPP is required when there is the need to ensure the highest level of identity assurance. IPP is also an alternative verification method for individuals who could not go through an online document verification process — for lack of computer literacy or credit history.

> *Fifteen percent of adults do not have a smartphone and 23 percent do not have access to broadband Internet at home.*
>
> *- Pew Research Center*

A remote form of IPP, virtual in-person proofing, has recently emerged. Virtual in-person proofing involves a videoconference with an employee of the biometric verification company, called a trusted referee.[26] The referee makes a comparison of the individual's physical features with a physical credential, such as a driver's license or passport.

[21] Biometric algorithms are considered biased if there are significant differences in how they operate when interacting with different demographic groups of users. Consequently, certain groups of users are privileged while other groups are disadvantaged. "What is Demographic Bias in Biometrics?," Mitek, April 15, 2021, https://www.miteksystems.com/blog/what-is-demographic-bias-in-biometrics?.

[22] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic Bias in Biometrics: A Survey on an Emerging Challenge," *IEEE Transactions on Technology and Society*, no. 2 (2020): pp. 89-103, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9086771.

[23] P. Grother, M. Ngan, and K. Hanaoka," Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NISTIR 8280, December 2019, https://doi.org/10.6028/NIST.IR.8280.

[24] "Precise ID Product Sheet," Experian, https://www.experian.com/assets/decision-analytics/product-sheets/precise-id-overview-product-sheet.pdf. Another example is Socure's Predictive Document Verification; see: Brenda Gilpatrick, "Three Reasons Machine Learning is Key to Predictive Document Verification," Socure, September 23, 2021, https://www.socure.com/blog/3-reasons-machine-learning-is-key-to-predictive-document-verification.

[25] ACLU, "Identity crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom," May 2021, https://www.aclu.org/sites/default/files/field_document/20210913-digitallicense.pdf.

[26] ID.me, "Virtual In-person Identity Proofing," https://www.id.me/business/virtual-in-person-identity.

However, remote verification may not work for citizens without a smartphone or access to the Internet.[27]

USPS Has Been Providing In-person ID Verification for Many Years

In-person proofing is a verification method the Postal Service has offered for a long time, well before technology providers started developing remote ID verification technologies. In 1975, USPS started providing the Passport Acceptance service to the U.S. Department of State. As part of the service, trained postal employees certify that the applicant has presented physical proof of citizenship. In 2003, USPS began verifying identities as part of a plan to provide citizens with a digital signature to conduct transactions with government agencies — however, the project was not successful.[28] Currently, customers need to show a form of identification to complete several postal transactions at a retail unit, such as renting a PO Box or picking up mail held up at the counter. Moreover, about 17,000 post offices support IPP for Informed Delivery subscribers who are unable to verify their identity online.[29] Management stated that the Postal Service plans on obtaining NIST IAL2 certification for its in-person identity proofing process by the end of 2022.[30]

In addition, USPS has recently piloted, on a relatively small scale, two other more complex forms of in-person services involving the collection of biometrics, in partnership with the GSA and the FBI. At the start of the pandemic, when GSA credentialing offices were closed, the Postal Service partnered with the GSA to conduct IPP for GSA's USAccess program in seven Washington, DC area post offices.[31] As part of the enrollment process, postal clerks at these locations collect, scan, and transmit identification documents and biometrics (picture and fingerprints) to GSA.[32] GSA and USPS have announced an expansion of the service from six to 22 locations in 2022.

In September 2018, the Postal Service initiated a partnership with the FBI to capture fingerprints for people requesting an identity history summary check (IdHSC).[33] As of March 2022, the service was available at about 180 postal locations throughout the country.[34] Instead of mailing a hardcopy fingerprint card to the FBI, customers can go to a participating post office or an FBI private sector partner location to have fingerprints taken and sent electronically to the FBI. The new system has reduced response times from more than three months to less than a week.[35] Postal clerks process a set of fingerprints in less than five minutes. In addition to these two services, several other IPP initiatives are in preparation, including with the GSA's Login.gov.

> *"USPS employees are very efficient. GSA normally processes enrollment in 30 minutes, but postal clerks got it down to 12 minutes. … That is faster than registrars in any other agency."*
>
> *– GSA representative*

[27] Pew Research Center, *Mobile Technology and Home Broadband 2021*, June 2021, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/06/PI_2021.06.03_Mobile-Broadband_FINAL.pdf.

[28] "In-Person Proofing at Post Offices (IPP) Program," *Federal Register 68*, No. 116 (June 17, 2003), https://www.govinfo.gov/content/pkg/FR-2003-06-17/pdf/03-15211.pdf, p. 35922.

[29] Customers bring required identification documents to a post office, together with a printed USPS barcode form. IPP is not offered if the closest post office is more than 50 miles from the address on an Informed Delivery account.

[30] The IAL2 level of assurance involves a physical comparison of applicant to facial-image photograph on strongest piece(s) of validated evidence or a biometric comparison of the applicant to the strongest piece(s) of evidence provided. Grassi, et al., *NIST Special Publication: Digital Identity Guidelines*, Table 5.3.

[31] USAccess provides access credentials (often known as Personal Identity Verification (PIV) cards) for federal employees and contractors at participating agencies. Identity proofing and registration requirements for the issuance of PIV Cards meet IAL3 requirements.

[32] Postal clerks validate and scan the documentation into the GSA's USAccess system but do not verify the authenticity of an applicant's identity documentation — the sponsoring agency does.

[33] FBI, "Pilot Program Allows Electronic Fingerprint Submission for IdHSCs at Select Post Offices," CJIS Link, October 15, 2019, https://www.fbi.gov/services/cjis/cjis-link/pilot-program-allows-electronic-fingerprint-submission-for-idhscs-at-select-post-offices.

[34] For a fee, the FBI provides individuals with an IdHSC that lists certain information taken from fingerprint submissions kept by the FBI and related to arrests and, in some instances, federal employment. An IdHSC may be required as part of a child adoption, among other uses.

[35] Chris Burt, "US Postal Service Fingerprint Biometric Service for Federal Vetting Surpasses 100 Locations," biometricupdate.com, November 3, 2020, https://www.biometricupdate.com/202011/us-postal-service-fingerprint-biometric-service-for-federal-vetting-surpasses-100-locations.

Government is Addressing the Urgent Need for Better ID Proofing

To address the need for better ID proofing, many agencies have partnered with private sector providers to implement the more secure remote verification methods discussed above. For example, Login.gov has implemented attribute validation and remote document validation through partnerships with verification companies including LexisNexis.[36] Some other agencies have gone one step further. For example, SWAs from more than 25 states have partnered with the verification company ID.me on the provision of remote document verification based on facial recognition. The IRS has implemented a similar, short-term plan to ask taxpayers to verify their identity with ID.me to access their online accounts on IRS.gov. For users not comfortable with facial recognition, they can opt for virtual in-person proofing (a live interview) instead.[37] Some SWAs are also using the IDV predictive identity verification solution. IDV (based on an Experian product) is a centralized ID verification for participating states. IDV returns an ID theft score to help assess whether a claim may be fraudulent.

In addition, government-wide initiatives have increased funding to support agencies' identity verification and fraud prevention efforts. The American Rescue Plan Act (ARPA) includes funds aimed at making government-wide, citizen-facing services more secure and effective. A number of ARPA-funded initiatives relate to ID verification and IPP. Grants approved in 2021 included GSA's development of in-person verification options and a verification API (Table 1).[38]

Table 1: Examples of ARPA-funded ID Verification Initiatives (2021)

Funding Vehicle	Beneficiaries	Scope
ARPA Fraud Grants	U.S. States	$140 million in DOL-administered grants supporting Unemployment Insurance Benefits fraud prevention – ID verification costs, data analytics, cybersecurity.
Federal Citizen Services Fund	GSA (Technology Transformation Services)	Development of an ID Verification API enabling ID verification with government authoritative sources.
Technology Modernization Fund	GSA (Login.gov)	The objectives of this $187 million award include the development of equitable ID verification tools and in-person options for vulnerable populations.

Source: OIG Analysis.

Related initiatives include the launch of an Initiative on Identity Theft Prevention and Public Benefits led by the ARPA coordinator.[39] In addition, in 2021, the PRAC created a Redress Working Group which focuses on preventing and addressing identity fraud in pandemic response programs.[40] Legislatively, the Improving Digital Identity Act of 2021, if passed, would create a comprehensive approach across federal, state, and local governments to address shortcomings in identity tools.

The Postal Service is not entitled to apply for the grants listed above. However, it Is important for USPS to stay abreast of and, where opportunities exist, engage in government-led secure ID promotion initiatives. Increased participation would give the Postal Service a better understanding of the whole-of-government approach

[36] Users provide a copy of an ID document, as well as their SSN and phone number, or have a confirmation code mailed to them. "Verify Your Identity," Login.gov, https://login.gov/help/verify-your-identity/overview/.
[37] The IRS has announced plans to replace these measures with an account registration solution based on GSA's Login.gov, to be implemented before the 2023 tax filing season. IRS Statement, February 21, 2022, https://www.irs.gov/newsroom/irs-statement-new-features-put-in-place-for-irs-online-account-registration-process-strengthened-to-ensure-privacy-and-security.
[38] An application programming interface, or API, is a software interface that enables data transmission between one software product and another.
[39] White House, "Statement of President Joe Biden on American Rescue Plan Oversight," May 17, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/17/statement-of-president-joe-biden-on-american-rescue-plan-oversight/.
[40] "Identity Theft in Pandemic Benefits Programs," PRAC, https://www.pandemicoversight.gov/our-mission/identity-theft-in-pandemic-benefits-programs.

to ID theft mitigation. USPS could then use this information to enhance its own ID verification efforts accordingly.

Potential Roles for the Postal Service in ID Verification

The need for stronger ID verification and the limitations of some verification methods create opportunities for the Postal Service to fill these gaps. This section highlights three concepts illustrating potential roles for USPS in the in-person and remote verification of identities.

We based the analysis of these roles on a study of the ID verification challenges government agencies currently face and interviews with government agencies and private sector providers. These roles also leverage some of the Postal Service's major assets: a vast retail network, databases of the nation's addresses, and experience with identity verification.

For each concept, we provide background information and a description of the service, and briefly address implementation considerations.

The Postal Service as Provider of In-person Proofing

The rise in identity theft and financial fraud has increased the need for enhanced ID verification standards for government programs. As such, IPP may grow in importance as a key method to verify an individual's identity.

Service Description and Rationale

Building on its experience providing IPP and the pilots with the GSA and the FBI previously described, opportunities may exist for the Postal Service to offer a portfolio of IPP services nationwide to the customers and employees of federal and state agencies including:

- In-person identity proofing. The Postal Service could progressively extend to other agencies the IPP services it currently provides at 17,000 locations for the users of its own services.[41] Postal clerks would collect and validate the authenticity of the ID document by comparing the application to the person on the photo ID, at the level of verification needed by the agency (IAL2 and potentially IAL3). As in the GSA pilot example, USPS would then transmit the data to the partner agency.
- In-person biometrics. The Postal Service could progressively extend the provision of in-person biometric services to include the 4,800 locations where it already provides the Passport Acceptance service. These locations — a subset of the 17,000 mentioned above — require specific terminals such as a fingerprint scanner and a space separate from the retail lobby.[42] As previously noted, biometrics-based capture and verification is a key feature of the most stringent assurance level, IAL3.

Beyond solely offering IPP in the confines of a physical post office, there may be an opportunity for USPS letter carriers to conduct at-home identity validation along postal routes. The Postal Service recently filed a patent describing how a carrier could use their mobile delivery device (MDD) to verify an identity then transmit information about the verification to other agencies.[43] France's Groupe La Poste already offers home identity verification. In France, it is one of three methods customers can choose from to create a postal digital identity, in addition to IPP at a post office and online verification.

IPP Could Serve Multiple Verification Purposes

According to the interviews we conducted with agencies, companies, and industry organizations, a nationwide IPP service could serve the public interest by addressing multiple verification needs. First, it could represent a fallback option for government customers who have failed remote identification verification, do not have easy access to a computer or the Internet, or simply prefer to go to a nearby post office to verify their identity. All citizens, especially disadvantaged segments of the population, would have an equal access to identity verification.

Second, IPP could be a strong verification method for agencies requiring the collection of biometric ID credentials or seeking ways to fill gaps in or fortify their identity verification processes. Login.gov users could verify their identity in-person at a local post office. The user would receive a QR code, go to their local post

[41] Clerks access IPP through the Retail Software System, which is in place in these 17,000 locations.
[42] The Passport Acceptance service is provided at a counter separate from the retail windows. The counter is generally located in a separate office with a door.
[43] U.S. Patent and Trademark Office (USPTO), *System and Method of Providing Identity Verification Services*, Patent Application 16/397901, filed on August 22, 2019, https://uspto.report/patent/app/20190260725.

BACK to COVER

office, and present ID documents to the postal clerk for verification.

Finally, IPP may be a convenient way for ID theft victims to recover their identity. Currently, there is no single point or central hub where victims could prove who they really are to all the agencies and organizations (such as credit reporting agencies) with whom they interact. Victims need to reach out to each of them separately and follow their specific redress process, which in some cases may already include IPP.[44] For this reason, the ITRC has called for the creation of a government-managed "fusion center." In the ITRC's vision, the fusion center would be a one-stop-shop access point to help victims regain access to government agencies' services. It would share ID theft alerts among federal, state, and local agencies, and with private sector partners (such as banks and CRAs). The fusion center could also help victims set up a specific identity recovery plan. The Postal Service could support the fusion center by validating victims' identities at the highest assurance level in postal retail locations, then transmitting that information to other agencies and private sector partners through the fusion center.

> *"Until we get to a point that every single person has Internet access, and is comfortable and able to use it, there is still going to be a need for in-person proofing."*
>
> *- James Lee, Chief Operating Officer, ITRC*

USPS's Retail Network is Well Positioned to Provide IPP Nationwide

Many of the ID verification companies and the government agencies the OIG interviewed highlighted several competitive advantages in having IPP services provided through the Postal Service's retail network.

For one, the Postal Service could build on the experience it has gained in verifying identities and its existing infrastructure and ID verification processes. The GSA credentialing and FBI pilots have demonstrated that additional government services can be provided effectively in the same space as the passport service and by the same trained clerks. In theory, economies of scope would help the Postal Service offer these services at a reasonable cost.

Moreover, the Postal Service has been designated as an essential service for the nation and an integral part of the federal response to the COVID-19 crisis. As such, its retail locations, unlike many other federal customer-facing facilities, remained open during the pandemic lockdowns.[45] Should a similar situation happen again, this could make USPS a welcomed backup network for agencies that require in-person proofing for some processes — such as SSA, IRS, or the Federal Emergency Management Agency.

Lastly, the Postal Service has an unrivaled retail footprint, with 17,000 post offices currently having the capacity to process IPP transactions. The breadth and reach of the postal retail network provide a unique opportunity for government agencies to expand their physical presence across the country and offer their customers expanded access to their verification services.

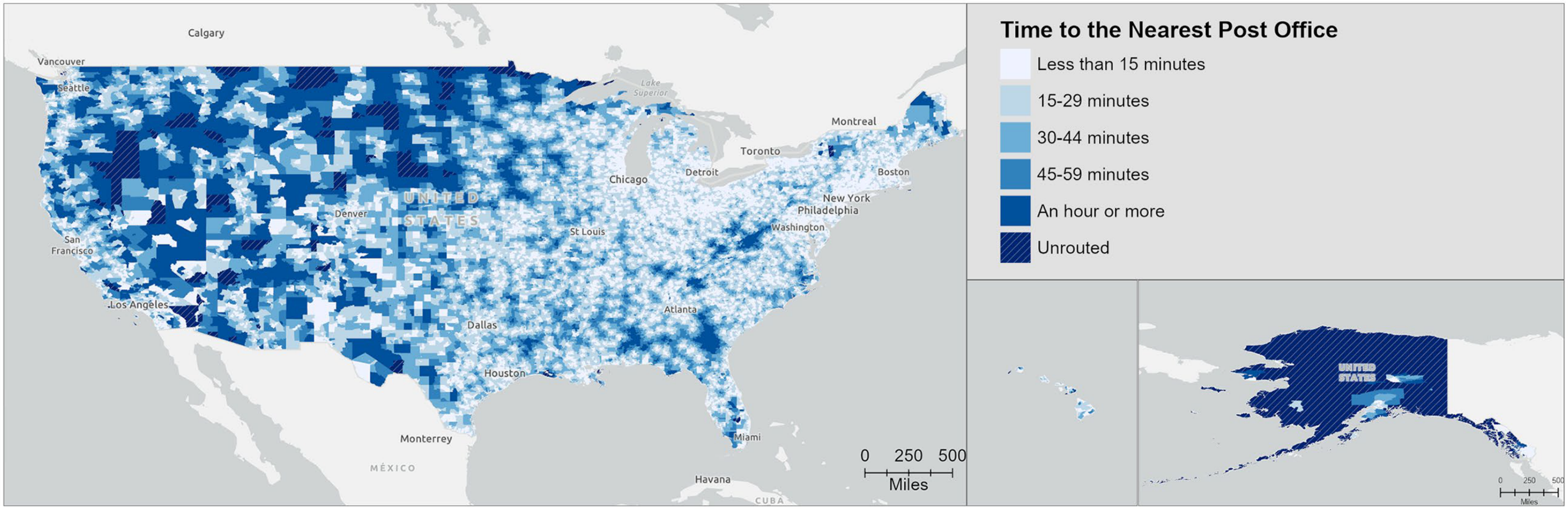
The Reach of the Postal Service's Retail Network Could Help Eliminate Government Deserts

To determine to what extent the postal retail network could complement the government's physical presence nationwide, we used GIS-based analysis. The purpose of our analysis was to measure how adding postal retail units would reduce the size of the so-called "government deserts." GSA considers "government deserts" to be areas where the nearest government credentialing location is at least a 60-minute drive away from a resident's home.

[44] DOL has stated that "if a future claim is filed under the victim's SSN, the claimant undergoes a secondary ID verification process (e.g., include an in-person reporting requirement or other expanded ID verification alternatives)." DOL Employment & Training Administration, "Advisory: Unemployment Insurance Program Letter No. 16-21," p. 10.

[45] See for instance "Social Security Offices Have Been Closed for Most of the Pandemic. That Effort to Protect Public Health has Wounded Some of the Neediest Americans," *Washington Post*, December 18, 2021, https://www.washingtonpost.com/politics/social-security-coronavirus/2021/12/18/0e3b9508-4bc1-11ec-b73b-a00d6e559a6e_story.html.

Figure 2: Driving Time to the Nearest Postal Retail Location With the Passport Acceptance Service



Source: OIG Analysis of Postal Service, GSA, and Census Bureau data.

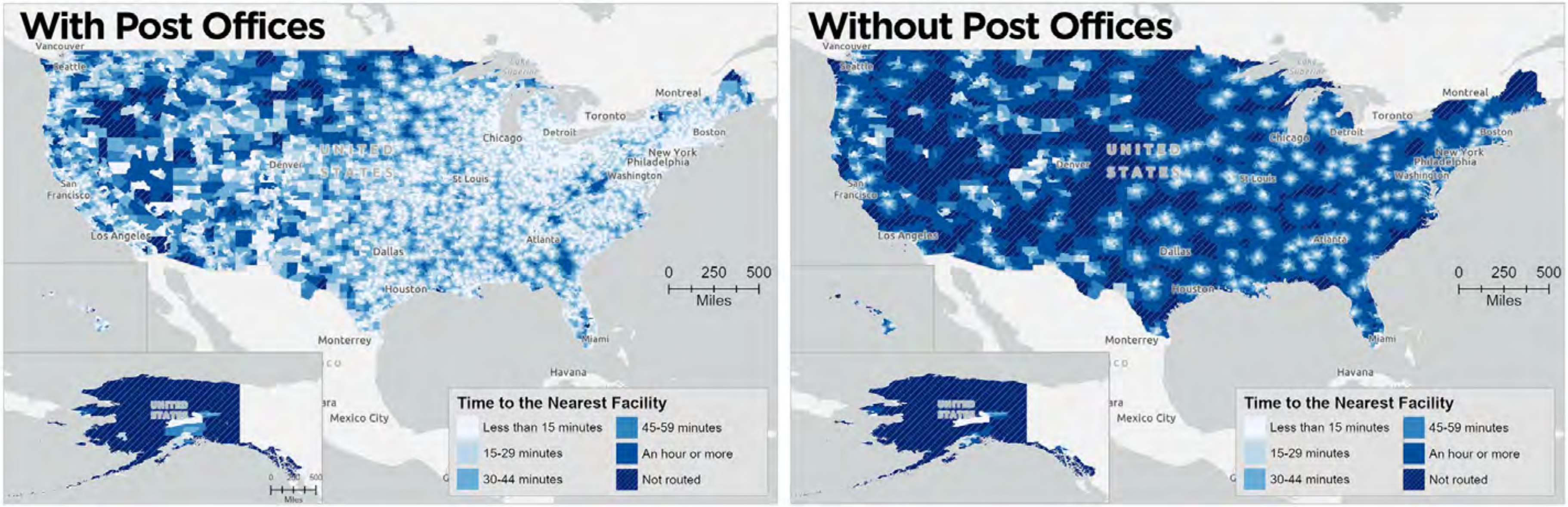
We first conducted GIS-based mapping and analytics to calculate the general population's average driving time to the nearest USPS retail location providing Passport Acceptance service. We used the 4,800 passport service locations as a proxy for a potential nationwide network of government service locations. OIG analysis showed that 70.6 percent of Americans live within a 15-minute drive of the nearest USPS Passport Acceptance location. Only 0.8 percent of Americans live more than 60 minutes from the nearest of these locations (Figure 2).

We then measured the potential convenience for government employees if the GSA credentialing service currently available in a sample of postal retail units were expanded to all 4,800 USPS Passport Acceptance locations, in addition to existing GSA credentialing offices. In this scenario, the share of government employees living more than 60 minutes from the nearest credentialing office would decrease from 23.8 to 0.6 percent (Figure 3). The average travel time would decrease from 46 to 14 minutes. Time savings would be larger in rural areas — 35 minutes compared to 28 minutes in urban areas.

While Figure 3 illustrates that time savings appear to be largest in large, rural parts of the nation, urban dwellers may also benefit. In the New York City metro area, for example, we found that many government employees living in suburban areas — not more than 30 or 40 miles from Manhattan — would save one hour or more going to the postal location. The main reason is GSA has few offices in these areas where the density of post offices is very high (see Appendix C).

Figure 3: Driving Time to the Nearest Credentialing Facility With and Without Post Offices

IF ALL USPS PASSPORT LOCATIONS PROVIDED THE GSA CREDENTIALING SERVICE, ONLY 0.6 PERCENT OF GOVERNMENT EMPLOYEES WOULD NEED TO DRIVE ONE HOUR OR MORE FOR THE SERVICE.



Source: OIG Analysis of Postal Service, GSA, and Census Bureau data.

Beyond GSA, many agencies have processes that include ID verification and fingerprint capture. For example, the United States Citizenship and Immigration Services must collect fingerprint records as part of the background check process on applicants for naturalization. Federal regulation requires state agencies to verify a Supplemental Nutrition Assistance Program applicant's identity to certify the household is eligible to participate in the program.[46] The level of complementarity between the postal network and each agency will depend on the number and location of that agency's customer-facing offices.

Implementation Considerations

Various operational and commercial factors will impact the Postal Service's ability to successfully scale up IPP services.

Execution Considerations

We interviewed several Postmasters in post offices offering Passport Acceptance and either GSA credentialing or FBI fingerprinting services. One of them suggested the need for a common scheduling service for all government services USPS provides, which would help balance clerks' time between government services and regular window duties.

Other organizations we interviewed, including an identity verification firm and the ITRC, highlighted the need for advanced training to ensure postal clerks who deploy IPP services can detect fraudulent documents. In addition, a "frictionless" IPP experience at post offices would include effective external communications

[46] See 7 C.F.R. § 273.2(f)(1) & (2).

to guide customers on what identity documentation they need to bring to appointments.

Finally, should USPS consider providing door-to-door IPP by carriers, there would be many factors to consider, such as ensuring the compatibility of this new function with carriers' regular delivery tasks.

Marketing and Commercial Considerations

The OIG did not attempt to measure the potential size of the IPP market. This will depend on the scope of services provided, the number of agencies USPS can partner with, and how effective the service is. Another factor will be the level of competition with private sector providers offering in-person proofing, either onsite or virtual (supervised by a remote operator).[47] In addition, legal limitations — which bar USPS from directly offering IPP to the private sector — also reduce the IPP market potential.[48] The Postal Service may wish to conduct additional studies and surveys to estimate the future level of demand for IPP.

The cost of IPP and the choice of a funding mechanism represent another related source of commercial risk. An ID verification company communicated that the price of in-person verification might be six times higher than the price of remote verification.[49] The price point may influence the agency's decision over the cost-benefit of offering IPP to their users. Since the Postal Service does not receive appropriations, to expand IPP, USPS would have to rely on a combination of alternative funding sources. These sources could include charging users — as does, for example, the Italian post — government funding, or seeking reimbursement from government agencies as part of an interagency agreement.

USPS as Validator of Identity Attributes

Government agencies that issue credentials — such as SSA, the Department of State, and State DMVs — maintain comprehensive databases containing users' PII, which they can validate. For example, when a driver's license applicant shows their passport at a state's department of motor vehicle facility, the clerk can connect in real time to the U.S. Passport Verification Service database. SSA's eCBSV service allows financial institutions to validate account holders' SSNs online. Banks or their technology partners submit a name, date of birth, and SSN number provided by an applicant, and SSA returns a match or no match result.[50] As the federal agency that maintains one of the most requested identity attributes — the nation's addresses — the Postal Service has the opportunity to play a role in this space.

Service Description and Rationale

[redacted] USPS could develop its capability of providing online name/address validation to government agencies.

A generic address validation scoring model could work as follows. As part of the ID verification process, the agency would electronically transmit to USPS the name and address of an individual. USPS would provide the agency a confidence level that this person lives at a specific address. A very high score — close to 100 percent — would indicate a high probability that a person lives at a specific address. When combined with the validation of other attributes, the value of the confirmed association of a name to an address could strengthen the ID verification process.

The Postal Service maintains current data on each delivery point in the country via its Address Management System (AMS), but the AMS does not associate addresses with individuals. To develop a method for calculating a confidence level indicator, the Postal Service could use other postal databases, such as

[47] "ID.me and Sterling Launch In-Person Identity Verification Service to Streamline Access to Government Services Nationwide," November 18, 2021, ID.me Insights, https://insights.id.me/press-releases/id-me-and-sterling-launch-in-person-identity-verification-service/.

[48] See discussion of legal limitations page 17.

[49] The indicative price points provided by that company were $25 and $4 per verified identity.

[50] SSA started rolling out eCBSV in 2020 pursuant to section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act ("Banking Bill"). In January 2022, SSA projected 280 million transactions in FY 2022, as more financial institutions were expected to join the system. "Notice of Open Enrollment and Fee Increase for Our Electronic Consent Based Social Security Number Verification Service," *Federal Register 87*, No. 10, pp. 2475-2477, January 14, 2022, https://www.federalregister.gov/documents/2022/01/14/2022-00638/notice-of-open-enrollment-and-fee-increase-for-our-electronic-consent-based-social-security-number, and SSA, "Information About eCBSV," https://www.ssa.gov/dataexchange/eCBSV/.

the National Change of Address (NCOA) or Informed Delivery.[51] If available, the number and type of letters or packages an individual has received over a certain period at a given address could be a good proxy for the likelihood that this person exists and lives at that address.

Interviews with verification companies highlighted a high degree of interest in using a name/address validation service from the Postal Service, in combination with other validation methods. They highlighted that the Postal Service would complement SSA's eCBSV as it would allow verification of people who do not have an SSN.

Implementation Considerations

Ensuring a high level of service speed and reliability, full compliance with the Privacy Act, and a clear communications policy are critical implementation considerations.

Execution Considerations

A fast and reliable name and address validation score hinges on the Postal Service's ability to successfully integrate its IT system with that of the agencies using the data to provide a real-time response to their queries. In addition, strengthening the processes the Postal Service uses to verify the identity of customers filing a Change of Address (COA) would be a prerequisite for ensuring users' confidence in the service.[52]

> *"IPP can be great if execution is done well, but an absolute disaster and create even more vulnerabilities if it is not."*
>
> *– Eva Velasquez, President and CEO, ITRC*

Finally, the Postal Service would need to comply with the Privacy Act of 1974, which generally prohibits the release of PII without an individual's consent unless certain exceptions apply to the disclosure.[53] Before providing a customer's name/address validation to another agency, that agency would first have to obtain the customer's permission to seek verification of the name and address association from the Postal Service. A clear definition of this process and the responsibilities of the agency and the Postal Service would help ensure full compliance with the Act. USPS will also have to develop a simple and transparent prior consent mechanism.

Marketing and Commercial Considerations

If poorly communicated to the public, the idea of "sharing personal information" — even among federal agencies — might induce privacy concerns. The Postal Service would have to clearly communicate to the public how the PII will be used and protected, as well as what the expected benefits are. Lastly, piloting the service with more than one government entity will help the Postal Service test the operational and commercial feasibility of this service.

USPS as Provider of Digital ID

In our first two examples of USPS involvement in ID verification, the Postal Service would leverage, respectively, its retail network and its address databases. In this last example, it would take advantage of another asset: its existing database of 47 million Informed Delivery subscribers.

Informed Delivery Users Hold Verified Digital Identity Credentials

To enroll in Informed Delivery, which gives subscribers a digital preview of their household's incoming mail, residential customers go to usps.com to create an account. Customers then complete an identity verification process that ensures that account is associated with a real and legitimate identity.[54] Users can verify their identity online, or in person by going to a post office. Currently, USPS's

[51] NCOA dataset includes approximately 160 million permanent change-of-address (COA) records. The COA records consist of the names and addresses of individuals, families, and businesses who have filed a COA request with the Postal Service. Business mailers use this information for address cleansing purposes — the process of standardizing, correcting, and then validating addresses — and updating customers' mailing addresses.

[52] U.S. Postal Service Office of Inspector General, *Issues Identified with Internet Change of Address*, Report No. 22-058-R22, April 12, 2022, https://www.uspsoig.gov/sites/default/files/document-library-files/2022/22-058-22.pdf.

[53] See: Privacy Act of 1974 (Privacy Act) (5 U.S.C. 552a).

[54] Informed Delivery® by USPS, USPS website, https://informeddelivery.usps.com/.

database contains the verified identities and addresses of a large and growing base of about 47 million Informed Delivery subscribers as of March 2022. From these subscribers, USPS collects personal information such as name, address, phone number, and email address. These USPS-verified identity credentials could potentially be used by Informed Delivery subscribers to prove their identities with partner agencies or organizations.

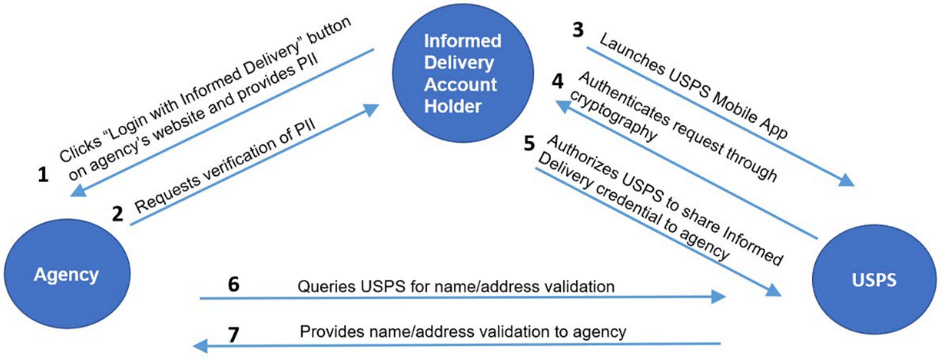
Other international postal operators, such as Australia, France, and Italy issue postal digital identities to the public for non-postal uses. For example, Australia Post's Digital ID can allow subscribers, among other things, to open a bank account, or access specific government services — in addition to picking up parcels in post offices.[55]

Service Description and Rationale

Informed Delivery subscribers could use their postal credentials for different verification purposes:

- As a single sign-on service - Instead of creating a new profile and verifying their identity whenever a new account is created with a government agency, users could reuse their existing verified Informed Delivery credentials. Clicking on a "Sign in with Informed Delivery" button on the government agency's website could allow them to prove their identity by consenting to the sharing of USPS-verified personal information with the agency.
- As a phone app - Informed Delivery subscribers' postal digital identity could be stored in a digital wallet accessed through their USPS Mobile® App. Subscribers could use the digital wallet to prove their identity online or in-person to access other USPS's services. Users could also use the wallet to access their accounts with other government entities accepting the wallet as an ID verification method (Figure 4). Fraud victims, for example, could use the app to reestablish their identity. If legally allowed in the future, the app could also be used by private sector companies. For example, a bank loan applicant could use the app to verify their identity with a financial institution.

Figure 4: Verifying Identify with an Informed Delivery-Based Digital Wallet


Informed Delivery Account Holder
Agency
USPS
1 Clicks "Login with Informed Delivery" button on agency's website and provides PII
2 Requests verification of PII
3 Launches USPS Mobile App
4 Authenticates request through cryptography
5 Authorizes USPS to share Informed Delivery credential to agency
6 Queries USPS for name/address validation
7 Provides name/address validation to agency

Source: OIG Analysis.

Using a verified Informed Delivery identity to create other government accounts could support current efforts to strengthen government agencies' ID verification methods. The service could make the verification process easier and more convenient, potentially speeding up the adoption of more secure verification processes.

However, when asked about the value of USPS potentially sharing Informed Delivery credentials, private sector companies the OIG interviewed generally provided mixed feedback. Some ID verification companies highlighted the value of the service and one of them expressed an interest in partnering with USPS to provide it. Otherwise, the general opinion was that the market for digital wallets is not yet mature, and the Postal Service should wait and see how the technologies and market needs for this service unfold before investing in its development.

Implementation Considerations

Unlike the two services discussed above, the Informed Delivery-based digital wallet is not part of the Postal Service's current ID verification portfolio. If USPS were interested in pursuing this idea, it would have to ensure it is technically feasible and conduct small-scale tests with interested agencies.

[55] Australia Post, Digital ID, https://www.digitalid.com/personal.

Execution Considerations

In the past few years, the process of verifying new Informed Delivery subscribers' identities has been strengthened. In particular, the Postal Service introduced a one-time numeric code verification method as a replacement for the knowledge-based questions it originally used. Sharing identity information with other agencies would involve additional technical steps, such as implementing safe security protocols for the exchange of data with agencies using the service.

In addition to these operational considerations, sharing Informed Delivery credentials would also need to meet Privacy Act requirements. The Postal Service's published "routine uses" — the list of the permitted disclosures of postal customers' records outside of the Postal Service — already allow disclosure of PII to "entities to which the customer wants to provide identity verification."[56] While the disclosure of PII to other government agencies may be allowed, the model still requires that customer consent be presented to the Postal Service before that data is disclosed to a government agency.

Marketing and Commercial Considerations

As already mentioned, technology providers are developing new technologies and standards — such as digital wallet standards — for the sharing of digital credentials. The Postal Service could monitor technology developments and assess the potential competitive advantages of an Informed Delivery-based solution. For example, the Postal Service could discuss with other agencies their interest in the service and conduct small-scale tests to assess the operational feasibility of this solution.

Given technical feasibility risks and uncertainties regarding future digital wallets standards, the provision of this service does not present itself as a short-term priority for the Postal Service.

Lifting Legal Restrictions Would Make These Services More Impactful

The Postal Service's ID verification services are non-postal services.[57] Under the regulatory framework defined by the 2006 Postal Accountability and Enhancement Act (PAEA), the Postal Service can provide non-postal services only to other federal agencies with which it can conclude interagency agreements. Interagency agreements provide for terms of service including reimbursement of costs the Postal Service incurs.[58] The Postal Service already provides passport, credentialing, and fingerprint services as part of such partnerships with the Department of State, GSA, and the FBI. The Postal Service may also provide services to state agencies, such as SWAs, which disburse funds — such as unemployment benefits — as part of federally funded programs.

The Postal Service Reform Act of 2022 (H.R. 3076) partially removed these limitations. It allows USPS to provide nonpostal services on behalf of any state, local, and tribal agencies. To be allowable, services should "provide enhanced value to the public," for example by raising their quality or accessibility.

However, the Postal Service would still be prohibited from providing ID verification services to the private sector, including, in most cases, ID verification companies. Allowing the Postal Service to offer ID verification services to the private sector, in addition to federal, state, and local government entities, could further increase the public interest and opportunities to monetize these services. Removing this barrier would require further legislation.

[56] See Routine Use #11 in Postal Service, Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*, February 2019, https://about.usps.com/handbooks/as353/as353apdx_007.htm.
[57] Verification services to companies would likely be considered as nonpostal, because they are not part of or ancillary to the processing or delivery of letters and packages. See 39 U.S.C. § 102(5).
[58] See 39 U.S.C. § 411.

Conclusion

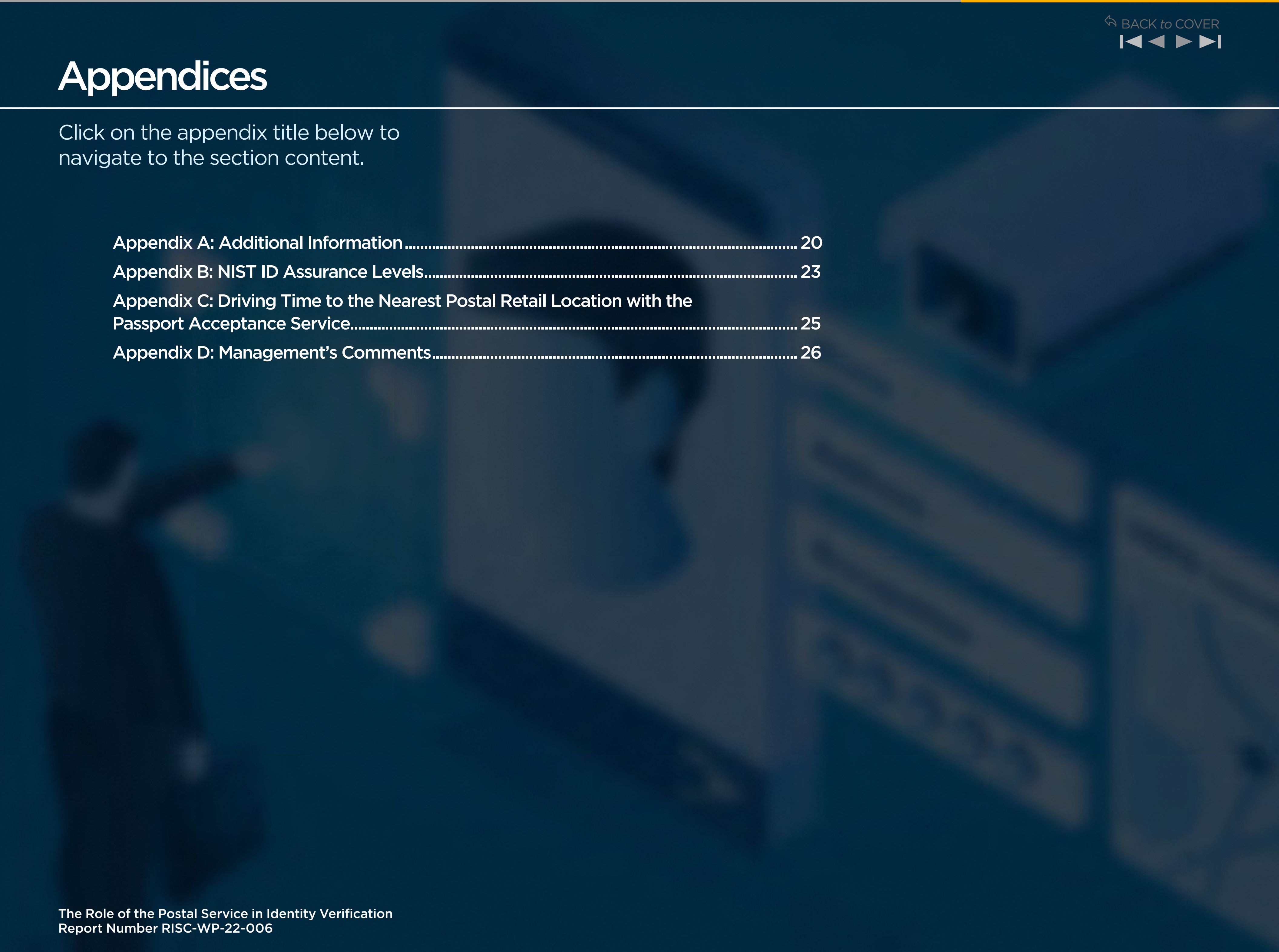
Based on feedback from OIG interviews with government agencies and private sector providers, two concepts appear to have a high potential in terms of their public interest value. By expanding IPP and providing online name/address validation, the Postal Service could contribute to filling service gaps in identity verification processes. Given the still evolving market and technology environment, the third concept — the Postal Service as provider of an Informed Delivery-based digital ID verification service — may not be a near-term prospect for the Postal Service.

As government and commercial players implement new ID verification strategies and partnerships, a window of opportunity is currently open for the Postal Service to help meet government agencies' needs for a broader choice of effective verification methods. To maximize this opportunity, the Postal Service should act swiftly. Finally, further legislative action allowing the provision of ID services to private sector businesses could allow the Postal Service to maximize the commercial and social value of these services.

BACK *to* COVER

Appendices

Click on the appendix title below to navigate to the section content.



BACK to COVER

Appendix A: Additional Information

Objectives, Scope and Methodology

The objectives of this paper were to:

1. Highlight the regulatory, technological, and competitive environment for providing digital identities (IDs) in the United States, and
2. Compare potential models for the provision of secure government digital IDs, including their complementarity with government networks, justification for use, and factors for successful implementation, for consideration by the Postal Service.

The scope of this project was an analysis of three types of identity verification service opportunities for the Postal Service:

1. Provider of identity proofing. The Postal Service would provide verification of ID documents, collect biometrics, and perform other document acceptance services on behalf of another agency.
2. Validator of identity attributes. The Postal Service would provide other agencies with validation matching names and addresses, using either Postal Service systems or in-person carrier verification.
3. Provider of Digital ID. The Postal Service could work with other federal agencies to explore whether USPS's 47 million Informed Delivery subscribers could use their postal credentials to securely access their other federal accounts.

We also reviewed past efforts from USPS and other government agencies to expand identity services over the past years.

To gather information for our analysis, we conducted a combination of desk research, interviews with government and private sector representatives, and geographic information system (GIS) analysis:

Desk research

- For background information on the topic of digital identity verification, we read a variety of reports, in particular from government agencies and their OIGs, news articles, as well as studies on ID verification technologies and market trends.
- To review the potential roles for the Postal Service in identity verification, as well as potential implementation issues, we analyzed relevant Postal Service memos, presentations, and databases such as the HR Biometric Onboarding Dashboard.

Interviews

- Between September 2021 and January 2022, we conducted 21 interviews, including:
  - **Postal Service managers** overseeing the development of digital and government services;
  - **Postmasters and clerks** who work at several pilot post offices where the USAccess or FBI credentialing services were provided;
  - **Government agencies** engaged with digital ID verification initiatives, such as Social Security Administration, General Services Administration, Veterans Benefit Administration, Treasury Inspector General for Tax Administration, Maryland Motor Vehicle Administration, and members of the American Rescue Plan implementation team;
  - **Industry organizations** Better Identity Coalition (BIC) and Identity Theft Resource Center; BIC also organized a discussion session for us with 55 of its members; and
  - **ID verification firms**.

GIS analysis

To analyze complementarity between the postal retail network and government customer-facing networks, the OIG conducted multiple routing analyses in ESRI's ArcGIS Pro Software. In these routing analyses, we calculated the travel time between each U.S. Census block group and different sets of identity proofing facilities in three scenarios:

- Scenario 1: The nearest postal retail location that currently offers the Passport Acceptance service;
- Scenario 2: The nearest government facility currently offering USAccess services;
- Scenario 3: Considering the combined Passport Acceptance and current USAccess networks, the nearest facility offering one of the two services.

Calculating the travel time from each block group to the nearest postal location currently offering passport services allowed us to measure the potential benefits of allowing them to offer other identity verification services.

By comparing the travel time from each block group from Scenario 2 to the travel time to for each block group in Scenario 3, we were able to calculate the potential travel time savings that government employees in need of identity verification through GSA's USAccess would incur if the service was also provided at the nearest passport postal location. Travel time was calculated based on the shortest driving distance from the geographic center point of each block group to the nearest facility.

Our analyses did not account for variations in driving conditions such as road congestion, weather, or time of day. Additionally, all three routing analyses used a 100-mile cutoff, meaning that any block group more than 100 miles from the nearest facility was not routed. Block groups are statistical divisions of census tracts generally defined to contain between 600 and 3,000 people. Block groups are also the smallest geographic level at which the U.S. Census Bureau publishes census data.

To produce maps for use in the paper, we placed each block group into one of six categories based on their travel time to the nearest facility. For each of the three routing scenarios, we categorized block groups as within 15 minutes of a facility, 15-30 minutes from a facility, 30-45 minutes from a facility, 45-59 minutes from a facility, 60 minutes or over from a facility, or not routed. We also produced maps showing the time savings from Scenario 3 as compared to Scenario 2 using these same categories. After categorizing block groups based on their travel time to the nearest facility, we assigned graduated color scales to these categories and selected areas of interest for each map. We examined these maps at both the national level and at the local level around major cities and their surrounding areas.

After completing our routing analyses, we enriched the data from those analyses with additional demographic data from the U.S. Census Bureau, accessed through ESRI Business Analyst. In addition to the travel time for each routing scenario, we added block group data for demographic categories including total population, labor force, working population, number of government employees, rural population, and urban population. Our demographic data came from the Census Bureau's *2020 American Community Survey*, except for urban and rural population statistics, which were sourced from the 2010 Census. The data allowed us to calculate the average travel time, median travel time, percent of the population within different travel times of the facility, and percent of the population that remained unrouted within each demographic group for all three routing scenarios.

The OIG conducted work for this white paper in accordance with the Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Inspection and Evaluation. We discussed our observations and conclusions with management on April 14, 2022, and included their comments where appropriate.

Prior Coverage

Title	Objective	Report Number	Final Report Date	Monetary Impact
Digital Identity: Opportunities for the Postal Service	Examine potential roles for the Postal Service in the digital marketplace, given the need for stronger identity authentication procedures.	RARC-WP-12-011	May 29, 2012	$0
Blockchain Technology: Possibilities for the U.S. Postal Service	Better understand blockchain technology's features and capabilities, as well as identify potential areas of interest for the Postal Service, including identity verification services.	RARC-WP-16-011	May 23, 2016	$0
Change of Address Identity Verification Internal Controls	Evaluate the Postal Service's identity verification internal controls for its Change of Address (COA) service.	MS-AR-18-005	August 24, 2018	$0
Step into Tomorrow: The U.S. Postal Service and Emerging Technology	Review some technological developments discussed in the OIG's previous work to assess which remain relevant today, such as secure identity management.	RISC-WP-21-007	August 26, 2021	$0

Appendix B: NIST ID Assurance Levels

In 2004, the National Institute of Standards and Technology (NIST) published the initial version of SP 800-63, Electronic Authentication Guideline. The latest major revision was published in June 2017.[59] Special Publication SP 800-63-A presents technical guidelines on enrollment and digital identity proofing for use by government and the private sector. It includes an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting an identity assurance level. The components of identity assurance in these Digital Identity Guidelines are:

- Identity Assurance Level (IAL): refers to the identity proofing process;
- Authenticator Assurance Level (AAL): refers to the authentication process; and
- Federation Assurance Level (FAL): refers to methods for exchanging authentication and attribute information data with a third party (called relying party), such as another agency.

For each of these categories, there are different levels of assurance (LOAs) that describe the strength of the identity assurance components — Level 1 is lowest and Level 3 is highest (Table 2). Agencies can select from these LOAs based on their risk profile (low, medium, or high impact) and the potential harm that could be caused by an attacker making a successful false claim of an identity or taking control of an authenticated account and accessing the agencies' systems. Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation;
- Financial loss or agency liability;
- Harm to agency programs or public interests;
- Unauthorized release of sensitive information;
- Personal safety; and
- Civil or criminal violations

Table 2: NIST Assurance Levels for the Proofing Process

IAL 1 (Lowest level)	Identity attributes, if any, are self-asserted or should be treated as self-asserted.
IAL 2	Either remote or in-person identity proofing is required. Requires identifying attributes in person or remotely using specified procedures.
IAL 3 (Highest level)	In-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation.

Note: CSP is a Credential Service Provider. A CSP is a trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use. NIST - Computer Security Resource Center, Glossary, https://csrc.nist.gov/glossary/term/credential_service_provider#:~:text=Definition(s)%3A,credentials%20for%20its%20own%20use.

In the NIST guidance, agencies are encouraged to conduct risk assessments to select the appropriate IAL and AAL levels for their services. If validated or verified personal information is needed to provide the service, the agency must examine the potential impacts of an identity proofing failure to determine if IAL2 or IAL3 is the most appropriate selection. The risk should be considered from the perspective of the organization and to the user since one may not be negatively impacted while the other could be significantly harmed.

At the IAL2 and IAL3 levels, the strongest form of identity verification is an automated comparison of a biometric characteristic (such as a facial image or fingerprints), collected and recorded as a reference, to a live capture of the same biometric characteristic. This method is optional at IAL2 level and mandatory at IAL3 level. Whenever a live capture of a facial image is used, NIST stresses there is a risk of impersonation, presentation, and spoofing attacks, and recommends the use of mitigating controls.

NIST also recommends the use of trusted referees to assist in the identity proofing and enrollment for populations that may not be able to meet or perform

[59] Grassi, et al., NIST Special Publication: Digital Identity Guidelines.

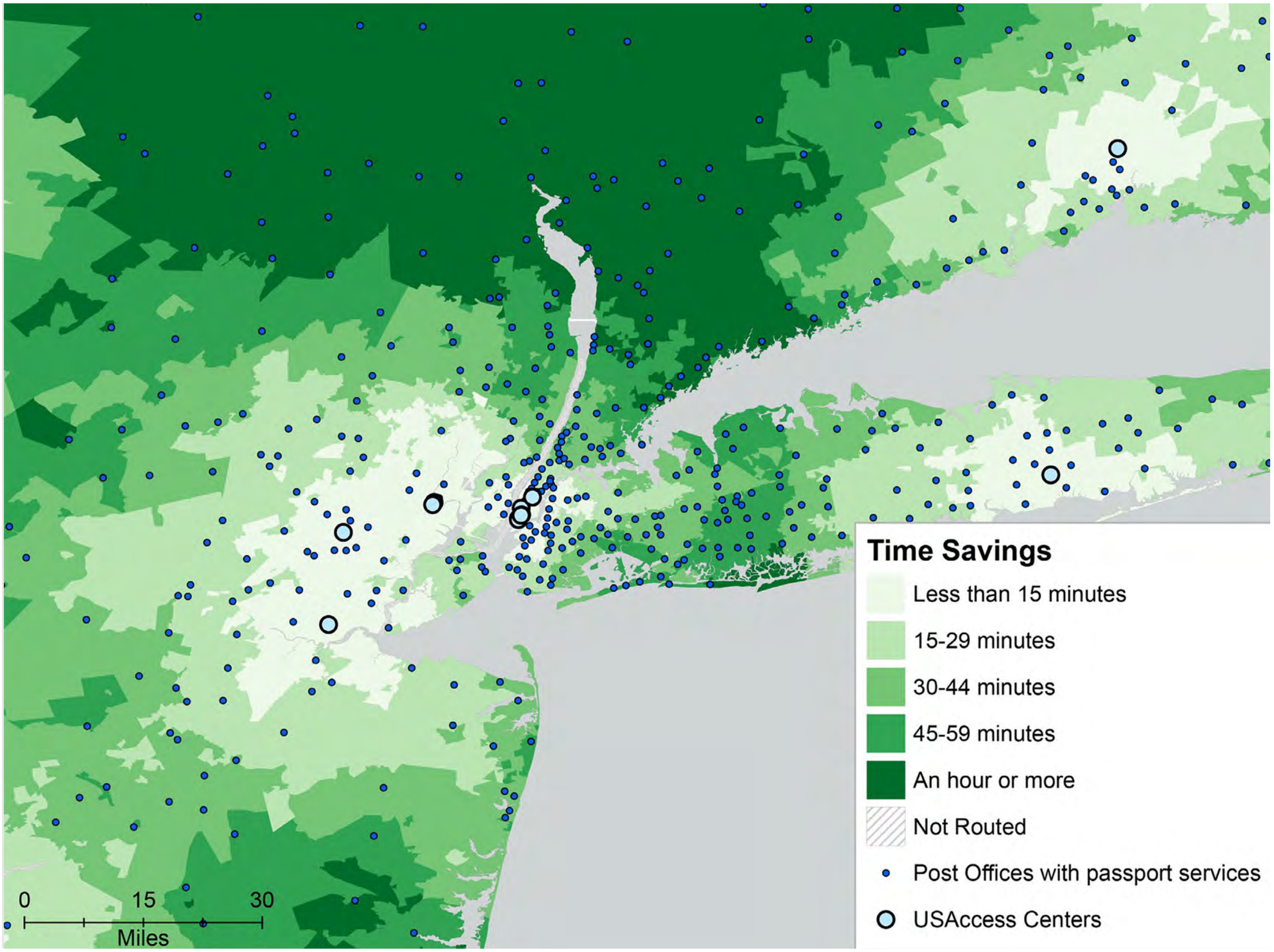
IAL2 and IAL3 identity proofing and enrollment process requirements. Such populations include, but are not limited to:

- Disabled individuals;
- Elderly individuals;
- Homeless individuals;
- Individuals with little or no access to online services or computing devices;
- Unbanked and individuals with little or no credit history;
- Victims of identity theft;
- Children under 18; and
- Immigrants.

Appendix C: Driving Time to the Nearest Postal Retail Location with the Passport Acceptance Service

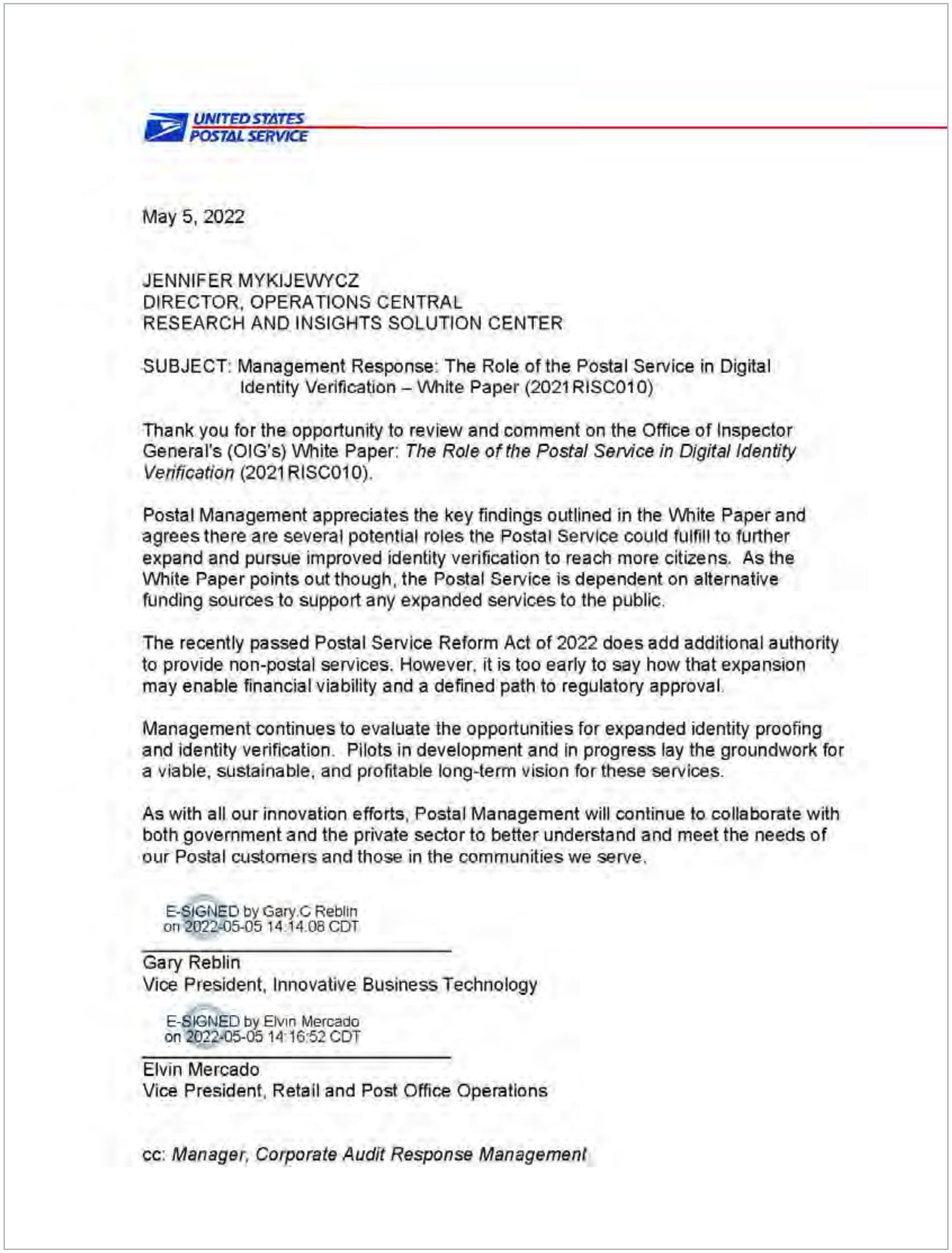
Figure 5: Driving Time Savings – New York City Area

IF ALL USPS PASSPORT LOCATIONS PROVIDED THE GSA CREDENTIALING SERVICE, MANY USERS IN RURAL AND SUBURBAN AREAS WOULD SAVE AT LEAST AN HOUR'S DRIVE.



Source: OIG Analysis of Postal Service, GSA, and Census Bureau data.

Appendix D: Management's Comments



UNITED STATES POSTAL SERVICE

May 5, 2022

JENNIFER MYKIJEWYCZ
DIRECTOR, OPERATIONS CENTRAL
RESEARCH AND INSIGHTS SOLUTION CENTER

SUBJECT: Management Response: The Role of the Postal Service in Digital Identity Verification – White Paper (2021RISC010)

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG's) White Paper: *The Role of the Postal Service in Digital Identity Verification* (2021RISC010).

Postal Management appreciates the key findings outlined in the White Paper and agrees there are several potential roles the Postal Service could fulfill to further expand and pursue improved identity verification to reach more citizens. As the White Paper points out though, the Postal Service is dependent on alternative funding sources to support any expanded services to the public.

The recently passed Postal Service Reform Act of 2022 does add additional authority to provide non-postal services. However, it is too early to say how that expansion may enable financial viability and a defined path to regulatory approval.

Management continues to evaluate the opportunities for expanded identity proofing and identity verification. Pilots in development and in progress lay the groundwork for a viable, sustainable, and profitable long-term vision for these services.

As with all our innovation efforts, Postal Management will continue to collaborate with both government and the private sector to better understand and meet the needs of our Postal customers and those in the communities we serve.

E-SIGNED by Gary.C Reblin
on 2022-05-05 14:14:08 CDT

Gary Reblin
Vice President, Innovative Business Technology

E-SIGNED by Elvin Mercado
on 2022-05-05 14:16:52 CDT

Elvin Mercado
Vice President, Retail and Post Office Operations

cc: *Manager, Corporate Audit Response Management*

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100