THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

CHALLENGES & IMPLICATIONS OF IDENTITY VERIFICATION IN COMBATING SOCIAL SECURITY BENEFIT FRAUD IN THE AGE OF AI

RYAN JOHN OOMMEN
SPRING 2026

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Cybersecurity Analytics & Operations
with honors in Cybersecurity Analytics & Operations

Reviewed and approved* by the following:

Tanusree Sharma
Assistant Professor of Privacy and Cybersecurity Informatics
Thesis Supervisor

Nicklaus A. Giacobe
Associate Teaching Professor of Privacy and Cybersecurity Informatics
Honors Adviser

* Electronic approvals are on file.

ABSTRACT

The Social Security Administration faces a growing identity verification crisis rooted in the limitations of its current infrastructure. Static identifiers originally designed for record keeping have evolved into digital authenticators which they were never intended to do. The reliance on knowledge-based and possession-based credentials has created exploitable gaps that can be leveraged by threat actors. This study argues that the failure of the current verification system is not just the increased volume of fraud cases, but fundamental flaws in the system's design from the start.

This study examines personhood credentials as an emerging verification framework to address this gap. Public sentiment and experiences with SSA identity verification systems are captured through a computational analysis of Reddit data and 13 semi structured interviews with individual participants. Findings revealed a pattern of user distrust and accessibility barriers resulting in fraud being viewed as an inevitable outcome of the current system. Participants expressed cautious optimism toward personhood credential-based verification as a potential solution while raising concerns around accessibility and AI-enabled threats.

This study concludes that no single verification mechanism can fully address the verification problem facing the SSA in isolation. Instead, layering personhood credential systems on top of existing infrastructure offers the most resilient path forward for security. Accessibility and governance must be priorities when structuring this new system. Building a verification system that confirms the humanness behind every interaction is a crucial step the SSA can take towards earning back the public's trust.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank all the individuals who made the completion of this thesis possible. First, I would like to thank my thesis supervisor, Dr. Tanusree Sharma, for her continued support and guidance throughout this process. Next, I would like to thank my thesis advisor, Dr. Nick Giacobe, for his guidance at the beginning of this journey. Last, I would like to thank all my family and friends whose encouragement and support allowed me to succeed. Most notably, my parents, Shane and Shiny, and my siblings, Aaron and Kayla. Without the support of these individuals, named and unnamed, none of this would have been possible.

Chapter 1

Introduction

Serving over 70 million beneficiaries annually and distributing trillions of dollars of lifetime benefits, the Social Security Administration (SSA) is one of the largest federal benefit systems in the United States (Social Security Administration, 2024). A large-scale benefit system, acting as a centralized data center of sensitive personal data, makes the SSA a high-value target for all types of cyberattacks. Among these attacks, fraud continues to dominate, most notably identity theft, synthetic identity creation, account takeover, and fraudulent benefit claims. These attacks have resulted in financial losses each year while undermining the public's trust in federal institutions.

The challenge at hand for the SSA is not just the presence of fraud, but instead the vulnerabilities of our current digital identity system. As essential services, such as Social Security, continue to transition into digital spaces, the challenge of verifying the identities of individuals in both a secure and reliable way has become more troublesome. The identifiers our system was built on, such as the Social Security number, were not designed to function as a secure authenticator. Static identifiers such as SSNs over time became digital keys to financial and government systems, as there were no other options. The problem resides in the possibility of a data breach; if compromised, they cannot be revoked or reissued at an effective scale. Once attackers obtain a static identifier, they are able to reuse compromised information indefinitely across institutions.

Current identity verification systems used across the Social Security Administration are very reliant on knowledge-based and possession-based credentials along with static identifiers

such as SSNs or other physical documents. Tools such as multi-factor authentication have been incorporated in different areas, yet these methods are not widely reliable. MFA and similar tools authenticate data attributes rather than confirm the existence of a real human individual behind a claim. An attacker does not need to be the real individual, they just need to have enough personal data to satisfy the system. As large-scale breaches continue to become more frequent, it has led to attackers having access to personal information and identifiers (Achten, 2023). The barriers of attack have become almost nonexistent, making bypassing existing verification mechanisms easier than ever.

To combat this problem of fraud, a clear distinction between validating information and verifying personhood needs to be addressed in our verification systems. Traditional identity verification models that were created to confirm that the user provided data matches what is stored in records fails to ensure that the user represents the real individual. As long as the data being presented appears consistent with stored records, unauthorized actors can access systems, leading to wrong individuals and synthetic identities successfully passing verification checks. Authentication failures is not the only reason for the growth and persistence of fraud, but also can be attributed to the limitations of the current verification system. As a result of this limitation, our outlook on digital identity verification must be adapted. Authenticating static identifiers that can be easily copied and breached has led the US to one of the worst fraud problems in its history (Newlin Disability, 2024). To address this worsening issue, an approach centered around uniqueness and human traits is needed. The adoption of personhood credentials fits that mold as it is a verification method that goes beyond confirming that a set of information is accurate, but that it is being presented by a real individual. Personhood credentials are unique to each individual as they leverage biometric traits and behavioral patterns. The use of verifiable

human attributes makes sure authentication cannot be easily stolen or copied. A change in verification to recognizing the human being behind the data can create a more fraud-resistant framework, offering a solution for struggling institutions such as the SSA.

Research Questions

By examining both public sentiment and direct user experiences, this study seeks to address the growing gaps and vulnerabilities in the Social Security Administration's identity verification infrastructure. To provide guidance throughout this investigation three research questions were sought to be answered: What are the prevalent challenges that users experience with the current Social Security Administration identity verification process? How do users perceive personhood credentials as a potential alternative to traditional verification mechanisms? What system requirements are essential to provide all users with a secure and accessible identity verification system process especially in a landscape with growing AI threats? To answer these three questions, a Reddit data scrape and a semi-structured interview stage was conducted. Results of both phases allowed for further computational and qualitative analysis of user experiences and perceptions.

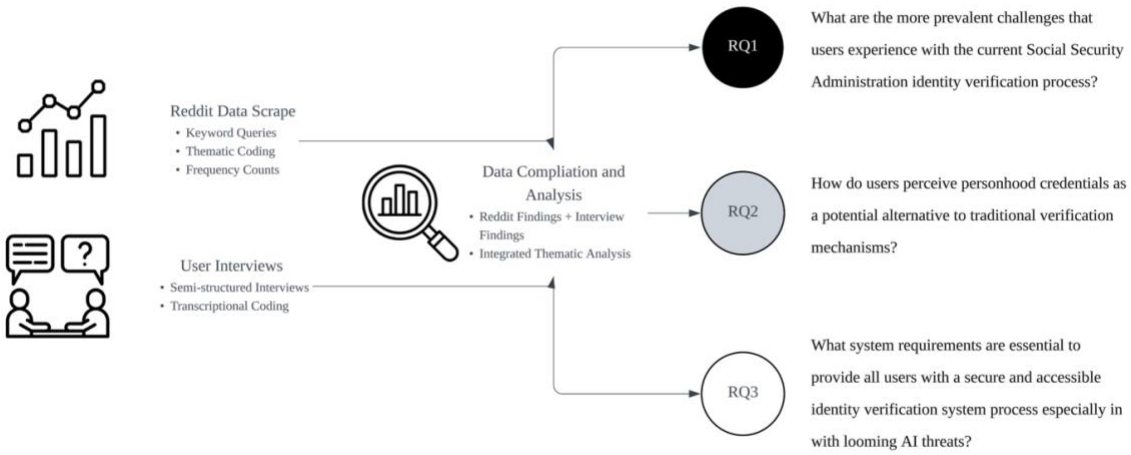

Figure 1: Study Workflow

Chapter 2

Literature Review

Social Security Fraud and Exploitation

In 1936, the United States created the Social Security Number (SSN), a move towards the future at the time. It paved a way to administer retirement and disability benefits, but as time has progressed its capabilities have evolved into much more. The modern SSN acts as a national identifier that individuals use across different institutions. These systems all incorporate SSN into their verification process, as it now serves as a unique identifier (Office of the Inspector General, 2023). Due to its widespread incorporation, the power of the SSN has grown tremendously, giving it the ability to obtain tax reporting documents or health records but also making it a valuable target for threat actors. According to the Social Security Administration Office of Inspector General (SSA OIG), the evolution of the SSNs has directly contributed to identity-related fraud schemes. In a congressional testimony, the SSA OIG emphasized that the original purpose for SSNs which was identifying earning records has been discarded (Office of the Inspector General, 2023b). SSNs have since evolved, now used in contexts they were never designed for such as authenticating individuals in digital environments leading to an increase in attackers taking advantage of identities. The increased roles required of the SSN outside its designed purpose along with a lack of verification safeguards can be directly attributed to this growing security problem.

These vulnerabilities go beyond SSNs, reflecting the weaknesses in static and knowledge-based identifiers. Static identifiers include dates of birth, driver's license numbers, taxpayer identification numbers, and other numerical identifiers used to identify individuals.

Knowledge-based authentication identifiers are reliant on the process of asking users questions based on their personal history. Once exposed, they are transferable and do not require any physical presence. Phishing campaigns or public record searching can lead to these verification methods being easily compromised and reused indefinitely.

The US Government Accountability Office (GAO) provided grounding for these concerns in the report "Employment-Related Identity Fraud: Actions Needed to Address Vulnerabilities and Better Measure the Problem" (GAO-20-492). They identified that nearly 1.3 million SSNs showed characteristics of potential employment-related identity fraud in tax year 2016 (U.S. GAO, 2020). Attackers were able to leverage legitimate SSNs and exploit real individuals' benefit systems. Threat actors demonstrated patterns as they attempted to exploit identifiers through systems that only require biographical data as proof of identity. The GAO further revealed another challenge across modern federal systems, inconsistent reporting and fraud definitions. Agencies do not have comprehensive and standardized processes for distinguishing fraud and improper payments. This directly creates issues for comprehensive assessments of fraud across individual cases. Yet the main issue is not administrative oversight, but the dependency of identity verification systems on static identifiers as authenticators. As more federal agencies such as the SSA transition to online services and remote portals, there has been little to no adaptation of verification mechanisms. In-person verification allows for physical documents and static identifiers to be complemented through context and human factors. However, in digital environments authentication is almost solely reliant on KBA and static identifiers without an in-person element. With a majority of personal data being widely available through data brokers or access to prior breaches, the barrier between security and impersonation is nearly non-existent.

There are several recurring fraud types facing Social Security Systems, one of the most frequent being beneficiary impersonation and account takeover. In these instances, threat actors obtain personal identifying information to access an individual's SSA account. Fraudsters use these compromised accounts to redirect benefit payments or initiate claims through online service portals (Office of the Inspector General, 2023b). Through large-scale phishing campaigns or data breaches, personal data is obtained and leveraged to the attacker's benefit. In addition to impersonation, the emergence of synthetic identity fraud has been very troublesome. Legitimate identifiers are combined with fabricated information to build new identities that are capable of bypassing verification measures. Synthetic identity schemes have become so intricate that some instances recorded by the US Department of Justice have been used to obtain government benefits and secure financial services (U.S. Department of Justice, 2017). Due to a portion of the identities being legitimate, detection methods struggle with distinguishing real claims from fake (U.S. GAO, 2017). This gap has allowed many of these schemes to persist for extended periods of time before they are discovered.

The impacts of identity fraud and the failure of current verification mechanisms go beyond just financial loss. The resources needed across multiple agencies to investigate these identity misuse cases are vast. Beyond the financial consequences, these attacks are capable of something much worse and irreplaceable, damaging public trust. Institutions like the SSA require the confidence and backing of the public; without trust, the system can deteriorate rapidly. As fraud continues to increase, the trust of its users decline, leading to an organizational strain to balance accessibility with fraud prevention. Altogether, the reliance on static identifiers and the lack of adaptation place government institutions in a tricky position. With personal information becoming more accessible through cyber breaches and databases, and attackers able to

impersonate legitimate beneficiaries, the exploitable gaps in the current system continue to grow. Understanding fraud attacks and threat vectors builds the foundation needed to evaluate alternative identity verification systems. Therefore, each method's trade-offs should be carefully evaluated as they are widely incorporated in our digital environments.

Identity Verification Mechanisms

Authentication methods in our current digital landscape vary based on the service being provided, leading to different forms of evidence being required based on the mechanism being used. These mechanisms are based off the knowledge the user knows, what the user possesses, or something the user is. At times, these measures can work to enhance security postures yet each method introduces its own vulnerabilities.

Knowledge-Based Authentication is one of the most widely implemented verification systems across different services and platforms. Through passwords or personal history questions, users are required to provide information that should only be known to them. The vulnerabilities KBA systems introduce are highly susceptible to memory or predictability issues. Users often reuse simple or generic credentials, failing to reach the complexity metrics that this system requires to verify succesfully. Additionally, the epidemic of personal data becoming widely available through breaches and public records has turned private knowledge into accessible information. Researchers Bosnjack and Brumen, examined the security and usability of KBA reflecting on this idea by saying “technological advances and users’ continuous bad management practices have allowed for an increase in security breaches over the last decade, prompting researchers and innovators to begin exploring possible alternatives” (Bošnjak & Brumen, 2019). As technology continues to develop and attackers continue to progress, KBA is increasingly viewed as a high-risk authentication method for secure systems.

Incorporated as a manual and automated process, document-based verification validates identification such as driver's license or passports. Document forgery and synthetic identity building have corrupted this traditional verification method as it has migrated to a digital environment. Verification conducted through uploading images or scanning documents have been crushed by the advances of digital editing tools and AI content generation. Synthetic identity construction introduces a grave problem to document-based verification as well due to systems not being technologically able to detect outliers. At financial institutions, 95% of synthetic identities are not detected during the onboarding process, costing an estimated $20-$40 billion across all industries (Simons, 2023). These threats have remained so successful in bypassing document-based security measures due to document verification being reliant on an attribute-matching system instead of a personhood confirming system.

Multi-Factor Authentication requires users to provide two or more forms of authentication. With an increased verification step, the difficulty of unauthorized access by mitigating single-point failures increases. Password-based systems are at less of a risk of exploitation with a multi-layered prevention method in place, improving overall authentication procedures. However, MFA is not a complete solution as there are inherent weaknesses and accessibility issues with the system. Components such as one-time passwords remain vulnerable to interception and phishing attacks (Descope, 2025). Similarly, man-in-the-middle and social engineering schemes have proven to remain effective even in systems that implemented MFA (Funkhouser, 2025). Usability and accessibility are roadblocks as well as MFA can place cognitive burdens on users due to timed components, leading to overall resistance. While MFA grants a significant improvement over single-factor authentication, it does not fully eliminate the risk of identity verification exploitations and failures.

Through the analysis of various literature, a recurring theme for all verification methods seems to prevail: shortcomings of security usability and scalability. For knowledge-based, document-based and biometric verification methods, a tradeoff between these three criteria is present, leading to numerous vulnerabilities. Instead of establishing and verifying a true proof of personhood, modern systems look only to verify the matching of credentials or traits. In large-scale public and private sector systems in which attackers can leverage stolen data, this becomes very problematic. This gap has driven interest in alternative models that move beyond static identifiers and toward more identity-centric approaches.

Personhood Credentials

Personhood credentials are an emerging verification mechanism in which human users are distinguished from automated bots and threat actors without requiring any sensitive personal information. Personhood credentials differ from traditional verification through a process that confirms the user is a real and unique person (Alder et al., 2025). In environments where the balance of privacy and security are at the utmost importance, personhood credentials support verification without disclosing personal information. As the difficulty of verifying human users online continues to grow, researchers view personhood credentials as a possible infrastructure of the future. This “proof-of-personhood” infrastructure has the ability to help digital platforms distinguish authentic individuals from bots and synthetic identities. Due to the growing advancements of automated impersonation and fraud, the interest in personhood credentials continues to increase. Personhood credentials offer a way to shift authentication away from reusable identity to confirming human uniqueness (Passport, 2026).

This system functions by users being issued a cryptographically secured token that represents human participation once verified. These credentials are generated through three

verification mechanisms: biometrics, social verification, and human effort verification. The issued credential demonstrates that the individual is a legitimate user without having to repeatedly submit identifying documentation. Zero-knowledge proof cryptography is usually implemented as it allows users to prove they are in possession of the credential without revealing the credential or other information from verification (Lavin et al., 2024). This preserves both organizational and user privacy across multiple interactions, mitigating vulnerabilities at different phases (Adler et al., 2025).

The first personhood credentials mechanism explored in the literature is biometric systems. These systems use an individual's biometric identifier such as an iris pattern or thumbprint scanning, during enrollment. Research in biometric authentication suggests that physical traits such as facial recognition or iris patterns can provide a strong signal of uniqueness (Abdullahi et al., 2023). However, limitations are present, including biometric data being irreplaceable if compromised and the risks of spoofing (ISACA, 2024). In this system, the biometric reference is converted into a cryptographic credential which is not stored to be reused. The UniqueID framework demonstrates how a decentralized biometric verification like such can enforce a one person to one credential system. This decentralized architecture reduces the risk that attackers could reuse stolen identity attributes to create fraudulent accounts (Hajialikhani & Jahanara, 2018).

The second approach would be social verification models, where participants confirm new users through a network validation process. Instead of access being granted by one authority, users are validated through relationships of trusted users. Individuals vouch for one another's authenticity allowing for algorithms to then analyze the network to identify clusters of fraudulent identities. By increasing the difficulty of creating large numbers of fake identities and

forcing attackers to build credible trust relationships to successfully carry out attackers, a social verification model deters the possibility of an attack (Siddarth et al., 2020). This approach does introduce its own challenges, as bias and collusion can infiltrate a trusted network.

The third and final approach is centered around human-effort-based verification mechanisms. CAPTCHA and similar systems have been integrated into verification systems for many years, yet the advances in AI have reduced their effectiveness (Kasada, 2025). New frameworks using the same cognitive element to confuse or highlight attackers have been proposed, using interactive challenges that require real time human participation. Participants are required to solve puzzles or attend sessions at a fixed time. This method relies on the fact that one person can only be in one place at once, exploiting those posing as real or synthetic identities. Although a great remodification of a traditional system, it is still vulnerable to human-assisted attacks and organized efforts.

Personhood credentials become extremely relevant when looking at the context of Social Security verification systems. At an institutional level, verification systems are heavily reliant on static identifiers and traditional verification mechanisms, such as one-time passwords. These methods are extremely vulnerable to being compromised, whether that be at the hands of organized attacks or AI threats. Personhood credential systems offer an alternative model in which verification is processed through uniqueness verification mechanisms, confirming the individual without the need for sensitive data. Personhood credentials is not just a theoretical system as its real-world applications have begun to grow. Worldcoin has implemented a PHC-based identity system called World ID, which uses an "Orb" iris scanner for personhood verification (World, 2023). Systems such as Worldcoin’s show the feasibility of one-person-one-

identity models at scale. Personhood credentials reveal a pathway for reducing fraud in high-stakes identity systems such as Social Security (Ide & Sharma, 2025).

As suggested by the literature, there is no one method that fully guarantees a secure and scalable digital verification process. Each methodology carries system-specific strengths and vulnerabilities. Biometric systems flourish when needed to decipher user uniqueness, but privacy concerns over stored information are a large risk. Social verification models leverage networks backed by trusted individuals, but may introduce bias, leading to large-scale coordinated attacks. Human-effort mechanisms require human participation in real time but can be exploited with attacks aided by human participation. Therefore, incorporating a hybrid approach that combines multiple verification strategies to counteract any single system vulnerability can enhance security across systems.

Impact of AI on Identity Fraud in Government Services

A new dimension of identity verification has been introduced with the rapid advancement of artificial intelligence in recent years. AI has demonstrated to be a strong tool in fraud detection and security automation, yet it introduces dangerous threats such as synthetic identity generation and deepfakes. This expanded attack surface that is widely available to malicious actors is particularly concerning within large-scale government institutions such as the Social Security Administration.

The barrier to entry for attacks like identity theft and fraud related schemes has significantly lowered due to generative AI tools. By harnessing AI capabilities, threat actors are able to fabricate identity documents and impersonate individuals at an extensive scale. Organizations like Europol have taken notice to this growing threat, warning that AI-generated synthetic content is increasingly being weaponized for social engineering and the bypassing of

identity verification systems (Europol, 2023). This threat poses an immediate risk for the SSA, specifically their phone-based identity verification. With voice cloning and AI generated voice replication becoming near impossible to distinguish to the average individual, audio verification infrastructure is a large vulnerability. Research published by the National Institute of Standards and Technology has highlighted that voice-based authentication systems are increasingly susceptible to spoofing attacks carried out through commercially available AI tools (Yamagishi et al., 2021). As the advancements of AI continue to improve and these tools become widely accessible, the reliability of traditional verification methods will continue to erode without adaptations.

Despite the dangers AI presents, meaningful opportunities for fraud detection and prevention are present as well. Trained based off behavioral patterns and historical attacks, machine learning models have demonstrated the ability to both flag and block suspicious activity. Going beyond traditional rule-based detection systems, AI driven systems offer a proactive layer of protection (Brooks, 2026). Additionally, developers continue to push AI boundaries further with one of example being IBM's Autonomous Threat Operations Machine (ATOM). This fully autonomous Security Operations Center technology leverages AI to contextualize threats in real time rather than reactively. By leveraging frameworks such as the MITRE ATT&CK Playbook and attacker behavioral patterns, continuous threat visibility is provided to organizations (IBM, 2026). Federal agencies have begun exploring AI-driven detection and prevention tools, yet implementation has been inconsistent and uneven across agencies.

Chapter 3

Study Methodology

Reddit Data Scrape

To obtain a holistic understanding of public sentiment and discussions around the Social Security verification landscape, a computational analysis of Reddit data was conducted. Reddit was selected as the primary data source due to its large library of detailed and experience-driven narratives related to government services and personal challenges. Reddit also allowed for access to unfiltered accounts of system interaction and personal anecdotes. The Python Reddit API Wrapper (PRAW) scanned Reddit for posts matching a set of keywords. Results were compiled in a structured Excel format for further analysis.

Data collection was initiated through a set of search queries that included both fraud-specific terms and broad terms related to system interaction. Phrases such as “social security fraud,” “SSI fraud,” “SSDI fraud,” “disability fraud,” “social security overpayment,” and “social security delay” were used. Queries were executed through multiple subreddits containing topics related to Social Security verification or benefits problems. Data was collected from r/socialsecurity, r/SSDI, r/Disability, r/personalfinance, and r/legaladvice. Problems across different contexts were captured by the combination of using both general and subject specific subreddits.

The analysis phase of this data scape used a hybrid approach, which combined coded themes and high-level categories. Thematic coding was used to provide summaries on each data point to gain a clear understanding on an individual case basis. Results were then organized into four primary categories: SSA Operations & Policy Discussions, Fraud, Payment & Benefit

Misuse, Fraud Accusations & Investigations, and Identity Verification & Login Issues. Data was assigned to categories of best fit, allowing for a structured analysis to better understand user sentiment. Frequency counts were generated by category to identify dominant patterns and areas of discussion.

Manual classification and review were incorporated as well to ensure both accuracy and the elimination of nuanced cases that couldn't be captured by automated data collection. The combination of tagging and manual review allowed for thorough analysis with a large dataset. The insights gained from this Reddit analysis served as a foundation for the interview phase and the identification of key challenges.

Final Category	**High-Level Theme**	**# of Posts**
Fraud, Payment & Benefit Misuse	SS Benefits Reduction	90
	SS Fraud Updates (Phone-Based / Direct Deposit)	1
Fraud Accusations & Investigations	SS Fraud Experience	57
	SS Fraud Accusation	1
	SS Fraud Possibility	1
Identity Verification & Login Issues	SS Identification Protocol Distress	32
	Foreign SS Verification Troubles	1
	SS Identification Protocol Distress (variant spelling)	1
SSA Operations & Policy Discussions	SS Question	3
	General SS Concern	3
	SS Fraud Updates	2
	Complaints about Government Benefits	1
	Government Security Criticism	2
	SS Fraud Question	1
(Uncategorized)		1
Total		**197**

Table 1: Overview of Statistics in the Social Security Reddit Dataset (N = 197)

User Interviews

In addition to Reddit-based data analysis, a qualitative interview study was also conducted. This interview study allowed for a better insight into user experiences with identity verification. The objective of this study was to gain a more comprehensive and substantial understanding of user perceptions with the current system while gauging user acceptance of personhood credentials as a possible solution. A total of 13 participants were recruited through this study using participant mailing lists and in person recruitment flyers.

Interview Procedure

All interviews were conducted remotely through Zoom being audio recorded and transcribed with participant consent. Each interview followed a semi-structured format using guided questioning while exercising flexibility depending on participant experiences. Interviews first began with a brief introduction outlining the purpose and format of the study. Interviews were structured into five main sections, the first being General Identity Verification Experience. Here, participants were asked to describe their understanding of identity verification and their overall background with methods such as one-time passwords and knowledge-based authentication. The interview then moved into the Government Services and Verification Processes section, where questions were tailored towards direct interactions with identity verification in government services. Questions asked participants for detailed answers on enrollment processes, types of verification required, frequency of re-verification, and any assistance needed during the process. Challenges of Fraud and Institutional Trust was the following section where participants reflected on experiences with fraud, trust in current systems, and privacy concerns. Participants were then introduced to the concept of Personhood Credentials in the Perceptions of Personhood Credentials and AI section. They were asked to

share their personal opinions of this system along with any prior exposure to similar technologies such as biometric verification. Participants were also questioned on their views of how advancements in artificial intelligence may impact this verification system. The culminating section was Preferences and System Design Recommendation, where participants were asked to propose improvements to current and future systems in response to challenges and concerns they had previously identified.

Data Analysis

Data collection then ensued by transcribing all recordings and compiling answers into a unified dataset after the completion of all interviews. A similar thematic approach that was applied to Reddit data was used for the interview data. This allowed for the identification of recurring patterns and perspectives across responses. Through manually reviewing transcripts, data was assigned codes based on emerging themes related to the research objectives. The findings from this interview study were compared with patterns observed in the Reddit dataset to identify consistencies between the differing experiences. By integrating both qualitative and computational processes, the overall validity of the research was strengthened.

Ethics & Data Protection

All participants provided their consent for both the study and audio recording through Google Forms and audio confirmation. Participants were informed of their right to withdraw from the study or abstain from answering any questions at any point in the interview. Additionally, they were assured that answers and quotes would be used in an anonymous manner, encouraging participants to speak freely about their experiences. Any questions about the interview procedure or content were answered directly during the interview session. Transcripts were stored in a secure university cloud environment for collaborative coding and

further analysis. Each participant received $25 in compensation after the interview, based on an expected interview duration of up to 60 minutes. The study was approved by our institution's ethical review board and data protection office.

Participant Demographic

This study included 13 participants ranging from 35 to 65 and older. 10 out of 13 participants were female with 2 male participants and 1 agender participant. Several participants reported disabilities such as blind or low vision with others reporting chronic illness/health-related disabilities, neurodivergent/cognitive disabilities, or mental health disabilities. Participants were all Untied States residents spread across the country. 11 out of 13 participants reported direct experience with the Social Security system voicing their challenges prior to the study.

ID	Age	Gender	Used SS?	SS Challenges / Concerns
P1	55–64	Female	Yes	Authorization issues
P2	55–64	Female	Yes	Identity verification process not secure or accessible; unclear next steps when logging in; confusing page wording and delays
P3	35–44	Female	Yes	Frustrating to navigate with a screen reader
P4	45–54	Female	No	No challenges reported
P5	35–44	Female	Yes	CAPTCHA audio options not working; difficulty reading printed/large print forms due to vision problems
P6	35–44	Female	Yes	Concerned that users without assistance cannot complete identity verification at all
P7	65+	Female	Yes	Cannot independently fill out forms
P8	45–54	Male	No	No personal experience; aware others have struggled with identity verification
P9	35–44	Male	Yes	Paper communications should be electronic (web portal/email) for screen reader accessibility
P10	45–54	Female	Yes	New login system (Real ID) is not accessible or blind-friendly; unable to complete registration
P11	35–44	Agender/No gender	Yes	Registration was difficult but the SSA system itself works well for accessibility once set up
P12	35–44	Female	Yes	No challenges reported
P13	55–64	Female	Yes	Uncertainty about what using the system means; used it for benefit information only, not yet applied

Table 2: Participant Demographics and Background

Chapter 4

Results and Findings

Reddit Data Scrape Results and Findings

The Reddit dataset consisted of various user posts related to Social Security experiences, fraud, identity verification, and administrative processes. Each data point was organized into one of four categories for further analysis. These four categories, Fraud, Payment & Benefit Misuse, Fraud Accusations & Investigations, Identity Verification & Login Issues, and SSA Operations & Policy Discussions, were used to capture various dimensions of user experience. Across the dataset, a pattern of user frustration and distrust was revealed. Complex interactions with system processes and individual experiences lead users to approach the current system with a level of uncertainty. With situations ranging from fraud to administrative errors to system failures, a negative reflection of current practices was revealed.

Fraud, Payment & Benefit Misuse

The category Fraud, Payment & Benefit Misuse represented the largest portion of the dataset, capturing a wide range of scenarios involving unexpected financial liabilities and benefit misuse. Many users had discovered substantial overpayment debts without any explanation, leaving the involved individuals to be held financially responsible for the debts. One user described this experience as both confusing and stressful when saying they “never saw a penny of that money… and have no idea what (they’re) supposed to do.” This problem went beyond just debt and liabilities in some cases, as users experienced their benefits suspended abruptly. System errors left beneficiaries without their promised benefit payments with little to no explanation. One user was incorrectly marked as deceased which resulted in their benefits

immediately being terminated. The extensive efforts required to gain access again has a severe impact on user's financial situations, with an individual describing their situation as "sick, ailing, and penniless." Similar incidents were very common in the dataset, demonstrating how systematic mistakes can result in large financial burdens worsening already troublesome situations for users. Another pattern identified was overpayment notices and confusion around processes. Inconsistent communication led users to describe experiences in which duplicate requests for documentation and prolonged delays in resolution were required, creating inconvenient loops. "If I filled this out…, why would I have to do it again?" said one user as they were required to resubmit already completed paperwork multiple times. The system's inefficiency was highlighted through a majority of user anecdotes as stress and uncertainty were common byproducts of their experiences. This category revealed that the risks of the SSA system are not just fraud and attacks but instead administrative mistakes and a lack of communication.

Fraud Accusations & Investigations

The Fraud Accusations & Investigations category highlights the impacts of fraud-related user interactions with the Social Security system. Accusations of fraudulent behavior or investigations with no underlying cause were common cases found in this dataset. Individuals often faced large financial and legal consequences as these accusations developed into further challenges. One user concerningly expressed they owed "well over 100,000 dollars" for being accused of faking a disability. Despite never being informed before the accusation, the user was the victim of further legal action, demonstrating the risk associated with these claims. Identity theft was another recurring theme as users commonly reported unauthorized access and misuse of their SSNs. Users discovered suspicious activity as SSNs were being leveraged for employment or benefit claims. Individuals were required to engage with multiple agencies, such

as the SSA and law enforcement, leading to a complex and tedious recovery effort. This section highlights the unique challenges of fraud within the SSA system, along with the landscape users must navigate to remediate the malicious activity that effected them.

Identity Verification & Login Issues

The Identity Verification & Login Issues category revealed the barriers preventing users from accessing Social Security services and successfully navigating the verification process. Even when legitimate documents were used, individuals commonly experienced failure of the verification system. Many individuals reported both system failures and lost records, resulting in the resubmission of documentation multiple times. This ultimately led to delays in processing and overall frustration with the system. One user described their entrapment in the system's loops when their documents were lost by the SSA, and they were required to restart multiple times. Others reported the process as both circular and backwards due to its dependence on requiring other forms of identification. Even those technologically proficient struggled with online verification systems as one user stated, "I can build a computer… but this online verification is impossible and frustrating." Barriers were particularly challenging for elderly and disabled groups, as accessibility enhancements were not present. This problem is not rooted in the technological ineptness of the interacting population but instead in issues at the verification system's foundation.

SSA Operations & Policy

SSA Operations & Policy categorized data by capturing administrative performance and policies, along with overall institutional trust. Frustration with application delays and a lack of communication were observed throughout the data. Users expressed dissatisfaction and distrust as these system inefficiencies were reflective of the current system's dysfunction. "Out of touch"

was how one user described Social Security leadership, arguing that policies and leadership statements were not aligned with current problems. The growing drift between policy makers and beneficiaries was reflected in this section, as those relying on Social Security did not feel heard in their continuous outcries. At the same time, some users acknowledged the need for stronger security measures in response to fraud. One user with a cybersecurity background emphasized that fraud "happens every day" and although inconvenient, stricter measures would help mitigate this problem.

Key Findings

This analysis across all four categories highlighted the connected challenges facing users of the Social Security system. Unexpected overpayments and benefit disruption emerged as a large concern, as it caused widespread financial instability. Although identity verification systems served as tools for fraud prevention, a large number of cases stressed they caused further barriers for legitimate users. Fraud was also a large challenge that a majority of beneficiaries faced, leading to complex resolution processes. Problems seemed to be worsened by administrative inefficiencies, with users frequently reporting delays and a lack of transparency. Ultimately, the findings of the Reddit data scrape highlight a growing tension between security and accessibility. An effective future solution must look to improve system performance in areas such as benefit disruption, fraud prevention and remediation, and administrative inefficiencies, leading to the rebuilding of public trust.

Challenge Area	Reddit Data Scrape N = 197 posts
Inaccessible verification process	34 posts 17% of dataset
Login & authentication failures	52 posts 26% of dataset
Fraud experience (personal/known)	91 posts 46% of dataset
Distrust in current system	13 posts 7% of dataset
Screen reader / CAPTCHA barriers	4 posts 2% of dataset
AI & emerging threat concerns	3 posts 2% of dataset
Administrative delays & errors	22 posts 11% of dataset

Table 3: Challenges Across Reddit Dataset

User Interview Results and Findings

Through conducting semi structured interviews, valuable user insight on the current identity verification system, along with their outlook on potential new mechanisms was gained. Following the collection of interview responses, findings were organized into thematic categories to allow for deeper analysis. A consistent pattern emerged throughout all interviews: perception of the current verification system being flawed. A tension between fraud prevention and system accessibility was highlighted, and an outcry for change was expressed by a large majority of particpants.

Current Verification Methodology Perception

Those relying on static identifiers and in-person verification expressed a lack of trust in the existing verification process. Knowledge-based verification was a major gripe with numerous

individuals, as they emphasized how easily this information can be accessed or compromised in today's digital environment. One participant explained, "If someone is really good with computers, they could probably find your social security number or your date of birth online, it's not that difficult anymore." "Private" information seems to be the opposite in today's digital landscape, completely undermining the current systems in place. Participants also expressed negative feelings towards the experience of current security measures as they seemed more procedural instead of secure. "It feels like they're just going through the motions…it doesn't actually make anything more secure" said one participant. This overall breakdown in trust completely undermines a system that is founded on the confidence of its users, leading to an unstable and unreliable system.

Fraud Experiences

Numerous participants described their experiences with fraud as an inventible event. Over 80% of participants were victims or knew someone who had experienced fraud. Participants consistently framed identity misuse as both common and difficult to prevent. The widespread availability of personal information and shortcomings of institutional security measures were the main vulnerabilities users highlighted. "Once information is out on the internet, it's there forever" said one user who had been a victim of fraud already. This reinforces the idea that current systems are reactive rather than preventative, identifying fraud only after damage has occurred.

Usability and Accessibility Challenges

Usability and accessibility challenges were among the most common themes found in user interviews. Participants described these processes as difficult to follow and repetitive, along with no real outlet for assistance. These issues were not isolated events, but instead consistent

patterns seen over the course of 13 interviews. "Even with my background and education, I felt like the process was almost impossible. The people on the phone were nice, but they couldn't really guide you through the process…you had to figure it out yourself" said one participant when describing their experience with the process. This process was described to be even worse for those with disabilities with one participant saying, "As a screen reader user, you have to click where it says audio challenge, but then to get back to click on hearing it, it's no longer in the same spot... It's like doing acrobatics on the screen. I hate it." A system designed to protect its users has led to a reduction in user trust due to the barriers introduced by design flaws.

Personhood Credentials Outlook

Personhood credentials were a foreign concept to most participants when asked about their perception of the system. After a brief definition and real-world examples, participants expressed cautious optimism. Many were receptive to the idea of moving on from systems that are reliant on static identifiers and towards verification methods based on uniqueness. One participant expressed their willingness when saying "Instead of repeatedly providing personal information, it would be better to have a digital ID system that uses biometrics like face and fingerprint, where you verify once and then reuse that securely." However, this optimism was exercised with some caution as concerns regarding privacy and accessibility arose. Participants were wary of the fact that those with disabilities may not be able to use biometric features, along with individuals with mental disabilities not being able to successfully navigate cognitive challenges. Similarly, the threat of AI was a common area of concern for participants, as many believed promising systems like personhood credentials could be compromised. One participant reflected on this threat when saying “There are real examples of scams where AI replicated someone's voice to trick others into sending money. Biometrics alone may not be enough in the

future, and systems may need a combination of methods to stay secure." Overall, participants recognized the potential benefits of alternative approaches such as personhood credentials but emphasized that for this system to be successful, transparency and clear safeguards are required.

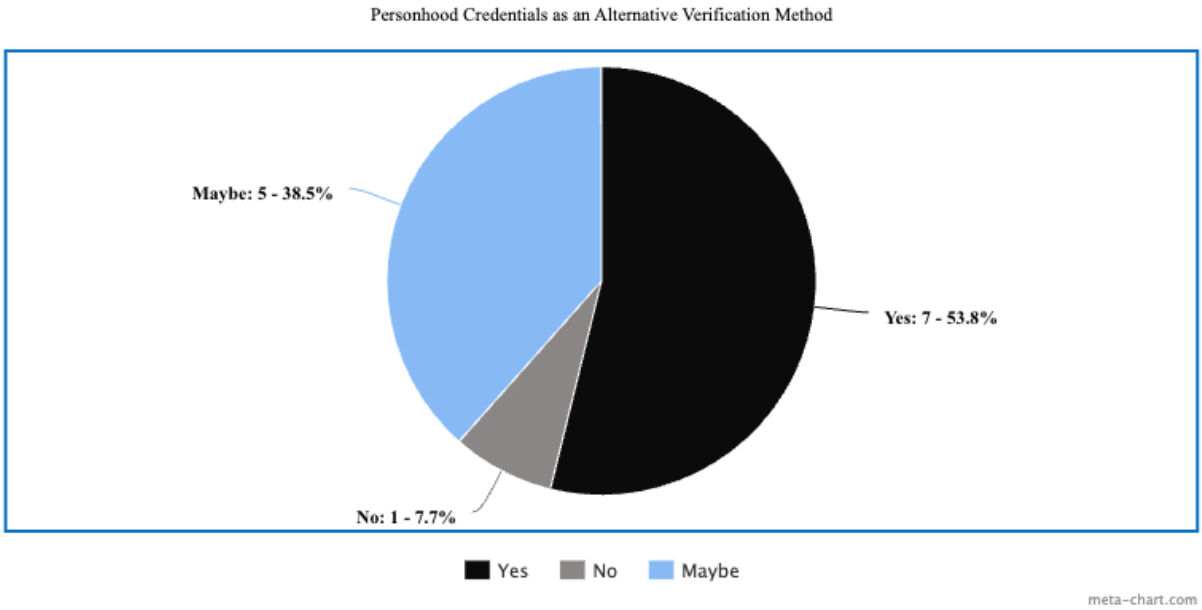

Figure 2: Acceptance of Personhood Credentials as an Alternative Verification Method

Design Recommendations

Across all 13 interviews, a consistent set of design priorities were recommended. The most widely agreed upon recommendation was the need for accessibility to be built into verification systems from the start. Many participants with disabilities ranging from vision impairments to cognitive challenges felt slighted in the current verification process. Although some services have measures in place already, many argued that they provided no real relief. One user attested to this when saying “there's a part that says if you're blind, click here, but it doesn't change anything." Similarly, many currently implemented verification mechanisms were called on to be more accommodating to various disabilities arguing that no single method works universally. Biometrics was among the most universally agreed upon with ten participants

calling for design changes to the system. One participant said "if someone doesn't have hands, they can't use fingerprints. If someone can't use their eyes, they can't use retinal scans. There have to be multiple options." Knowledge based authentication was recommended to be removed or reduced in use by eight participants with a user calling for it to be assigned “to the garbage bin of history." Changes of extended time windows and improved autofill functionality were recommended for faulty one-time password verification systems. Finally, a majority of participants wanted to see the reduced reliance on in-person verification due to travel barriers and security concerns with one participant pointing on that offices can be "hundreds of miles away” for some users.

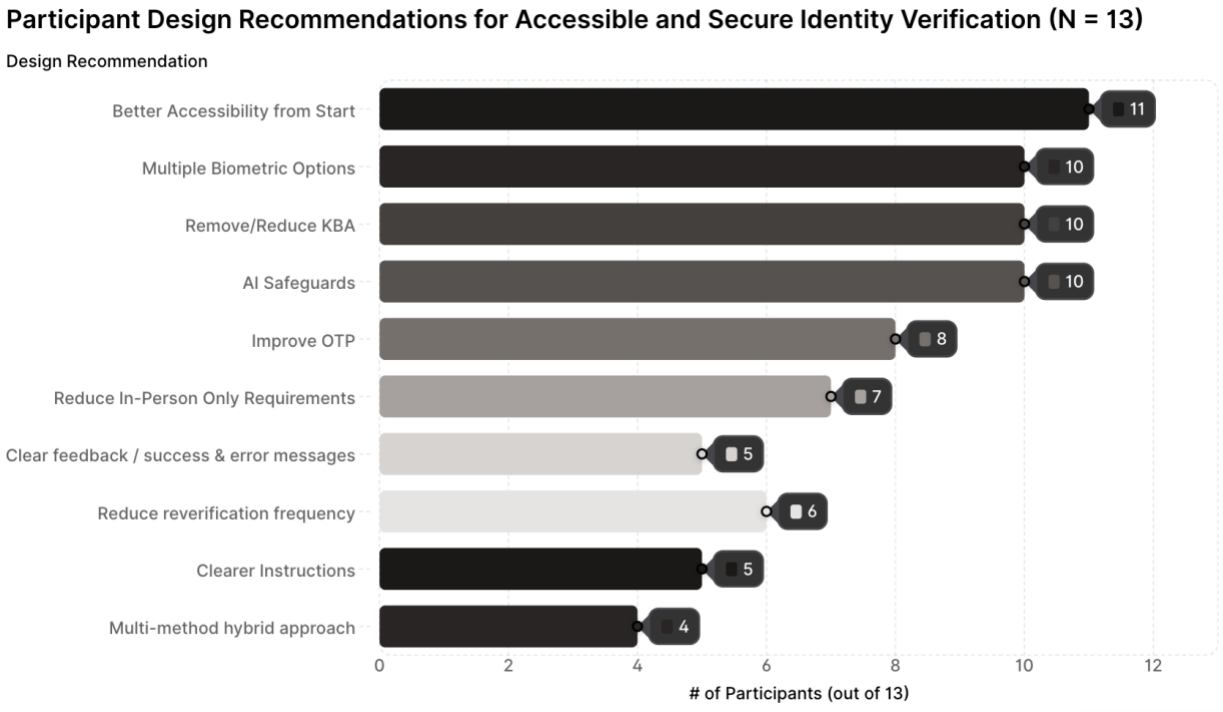

Figure 3: Participant Design Recommendations

Key Findings

Participants across the thirteen semi-structured interviews reflected a consistent dissatisfaction with the current identity verification system. Across the board, current verification methods were reviewed as flawed, lacking the necessary accessibility and security measures needed to be successful.

Challenge Area	User Interviews N = 13 participants
Inaccessible verification process	9 participants 69% of sample
Login & authentication failures	13 participants 100% of sample
Fraud experience (personal/known)	11 participants 84% of sample
Distrust in current system	10 participants 76% of sample
Screen reader / CAPTCHA barriers	5 participants 38% of sample
AI & emerging threat concerns	10 participants 76% of sample
Administrative delays & errors	5 participants 38% of sample

Table 4: Challenges Across User Interviews

Chapter 5

Discussion

The findings of this study highlight one conclusion: the SSA's current identity verification system is failing structurally. Static identifiers and traditional verification mechanisms were not designed for authentication purposes in large-scale digital environments. Users in both the Reddit data along with interview participants described that these breaches and failures were not just isolated incidents but instead inevitable outcomes of using the current identity verification system.

Data Patterns Explored

Reddit analysis revealed a pattern among users, fraud and administrative errors were not only common but indistinguishable from one another. Financial harm and confusion were common byproducts of systematic failures; the system designed to protect its users, has lost all precision needed to do so. The GAO's finding that 1.3 million SSNs showed characteristics of employment-related fraud in a single year (GAO, 2020) becomes more troubling in this light. This number of cases represents just the tip of a much larger failure that the SSA's own processes struggle to measure consistently. Interview data contextualized this further, as over 80% of participants had a direct or relational experience with identity misuse. Yet, participants were not outraged but numb as occurrences such as identity theft have become normalized and inevitable events. Users do not expect the system to protect them and are instead managing risk individually and reactively. Similarly, the shortcomings of accessibility were revealed in both datasets. Security measures designed without accessibility principles were a common problem

for those with sight and hearing deficiencies. A screen reader user describing CAPTCHA navigation as "doing acrobatics on the screen" illustrates how accessibility is currently treated as an afterthought. For a federal benefit system tailored to elderly and disabled populations, the gaps in accessibility are ethically inexcusable. A crisis is on the verge of breaking out as a benefit institution that relies on individual trust has severely damaged its user relations.

Literature and Data Relationship

Tradeoffs between usability, security, and scalability were uncovered through the literature reviewed verification mechanisms. Users experienced these tradeoffs using systems such as knowledge-based authentication, document-based authentication, and multifactor authentication. Some participants went so far to even say verification methods such as knowledge-based authentication are practically useless due to the information it relies on being widely accessible. This directly correlates to Bosnjak and Brumen's assessment, as the psychological security that authentication is meant to provide has already collapsed even where the technical mechanisms remain in place (Bosnjak & Brumen, 2019). Personhood credentials literature echoes that the current problem in our identity verification landscape would be the blurred line between validating data and verifying personhood (Adler et al., 2025). Without even being introduced to this concept revealed in the literature, participants commonly stressed similar themes. A preference for a model that requires one verification with a secure reuse mechanism was expressed by numerous users. However, the caution offered by the literature did resonate with interview data. AI-enabled threat actors proved to be a real concern among users, with a small majority reflecting on personal fraud encountered with similar tactics. Similarly, warnings that biometric systems must require ongoing evolution to remain effective against emerging attacks have become more urgent as generative AI becomes widely accessible. Thus, no single

mechanism, even personhood credentials, has the ability to be completely successful isolated. Instead, a hybrid infrastructure combining the strengths of multiple verification methods offers a resilient defense strategy.

Future Design and Implementation

This path forward calls for the layering of personhood credentials infrastructure on top of existing systems instead of full-on replacement. A hybrid model would allow for the SSA to introduce a foreign personhood credentials system reliant on biometrics, network validation, and human effort challenge verification while retaining traditional methods to fall back on. Not only would this infrastructure reduce the logistical burden of a completely new rollout, but it would also allow each system to complement the others based on individual situations and accommodations. Through mirroring existing approaches taken by organizations such as Worldcoin's World ID, the one-person-one-credential methodology could be introduced at scale. In this system, accessibility cannot be a secondary consideration, but instead future system's must be built with accommodations as a priority. Engaging with advocates of disabled communities to understand problems along with accessibility researchers in design processes from the earliest stages will eradicate problematic accessibility gaps. Governance of this new methodology must improve as well to bridge administrative weaknesses. Adopting real time fraud notification systems similar to those of financial services would transform protection from reactive to proactive. Improving communication along with creating trusted troubleshooting outlets, would improve the verification process for both existing and first-time users.

Limitations

Limitations for both Reddit data and user interviews were present during this study. The Reddit dataset overrepresents users who experienced problems with SSA verification systems, as

those with positive reactions are less likely to post to an online forum. Similarly, the sample size of 13 interview participants was a smaller study. Participants were recruited through a single recruitment channel, leading to a similar participant pool. Additionally, participants had little to no technical exposure to personhood credentials, leading to different concerns or hesitant support.

Future Research

A larger-scale study that represents the large majority of SSA beneficiaries would allow for qualitative results leading to more concrete findings. From there, pilot testing personhood credentials enrollment with users of varying technical backgrounds would allow for this concept to be deployed beyond just theory. Finally, tracking the performance of institutions with adopted verification systems would give both researchers and policy makers real-world evidence needed to transform theory into action. As the technology of these systems continues to develop, so do attackers and threats making further research imperative to protect our institutions and individuals.

Chapter 6

Conclusion

The findings of this study allow for a clear conclusion that the Social Security Administration's current identity verification infrastructure is not equipped to meet the demands of the modern digital landscape. Critical mechanisms such as static identifiers were never designed for authentication purposes leading to a fraud crisis that has affected numerous beneficiaries. Reddit data and interview participants were reflections of a population that does not expect protection from a system meant to serve them. The literature reviewed coupled with the data collected agree that no one verification mechanism can address this problem in isolation. Each carries tradeoffs in areas such as security, usability and scalability leading to vulnerabilities that can be exploited. Personhood credentials offer a meaningful step in the right direction by transforming verification from what an individual knows or possesses into confirming that the user is a real and unique person. However, even this promising model requires continued research and evolution to combat advancing AI threats.

Therefore, the path for a stronger and more resilient verification system does not call for the full replacement of existing systems but the layering of personhood credential infrastructure alongside current methods. Accessibility must be a priority when structuring this new system as a federal institution that primarily serves elderly and disabled population must meet this obligatory standard. Improved administrative communication and transparent governance would help bridge the ongoing tension between administrative and users. Altogether, these measures would build a hybrid approach that offers a viable framework for restoring both security and public trust. The SSA's benefit system runs on the confidence of the people it serves. Moving

toward verification systems that truly confirm the humanity behind every user in each step is a crucial phase in rebuilding public trust.

BIBLIOGRAPHY

"Autonomous Threat Operations Machine (Atom)." *IBM*, 2026, www.ibm.com/services/autonomous-threat-operations.

Abdullahi, S. M., Sun, S., Wei, N., & Wang, H. (2023, November 13). *Biometric template attacks and recent protection mechanisms: A survey* . Science Direct. https://www.sciencedirect.com/science/article/pii/S1566253523004608

Achten, A. (2023). *Identity Theft Resource Center 2023 Annual data breach report reveals record number of compromises; 72 percent increase over previous high*. Identity Theft Resource Center. https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/

Adler, S., Hitzig, Z., Jain, S., Brewer, C., Chang, W., DiResta, R., Lazzarin, E., McGregor, S., Seltzer, W., Siddarth, D., Soliman, N., South, T., Spelliscy, C., Sporny, M., Srivastava, V., Bailey, J., Christian, B., Critch, A., Falcon, R., … Zick, T. (2025, January 17). *Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online*. arXiv.org. https://arxiv.org/abs/2408.07892

Bošnjak, Leon & Brumen, Bostjan. (2019). *Examining Security and Usability Aspects of Knowledge-based Authentication Methods*. 10.23919/MIPRO.2019.8756655.

Brooks, Chuck. "Why Proactive Cybersecurity Is Essential in the AI Era." *Forbes*, 23 Mar. 2026, www.forbes.com/sites/chuckbrooks/2026/03/23/why-proactive-cybersecurity-is-essential-in-the-ai-era/.

Captcha's demise: Multi-modal ai is breaking traditional bot management. Kasada. (2025, March 27). https://www.kasada.io/captchas-demise-multi-modal-ai/

"Chatgpt - the Impact of Large Language Models on Law Enforcement." *Europol*, 27 Mar. 2023, www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement.

Employment-Related Identity Fraud: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks. U.S. GAO. (2020, May 6). https://www.gao.gov/products/gao-20-492

Funkhouser, A. (2025, January 28). *Multi-factor authentication (MFA) bypass through man-in-the-middle phishing attacks*. Netskope. https://www.netskope.com/blog/multi-factor-authentication-mfa-bypass-through-man-in-the-middle-phishing-attacks

Hajialikhani, M., & Jahanara, M. (2018, June 20). *Uniqueid: Decentralized proof-of-unique-human*. arXiv.org. https://arxiv.org/abs/1806.07583

Highlights of a Forum: Combating Synthetic Identity Fraud. U.S. GAO. (2017, September 15). https://www.gao.gov/products/gao-17-708sp

Ide, A., & Sharma, T. (2025, February 22). *Personhood credentials: Human-centered design recommendation balancing security, usability, and Trust*. arXiv.org. https://arxiv.org/abs/2502.16375

Identity thief sentenced for using a new form of fraud "synthetic identities." U.S. Department of Justice. (2017, April 28). https://www.justice.gov/usao-ndga/pr/identity-thief-sentenced-using-new-form-fraud-synthetic-identities

Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G., & Krishnamachari, B. (2024, August 1). *A survey on the applications of zero-knowledge proofs*. arXiv.org. https://arxiv.org/abs/2408.00243

Office of the Inspector General. (2023, May 30). https://oig.ssa.gov/news-releases/2023-05-30-the-social-security-number-the-lynchpin-to-identity-theft/

Phishing-resistant MFA: How it works and why you need it. Descope. (2025, January 24). https://www.descope.com/learn/post/phishing-resistant-mfa

Proof of personhood explained: How it works, who's building it, and why it matters now. Passport. (2026, February 26). https://passport.human.tech/blog/proof-of-personhood-explained-how-it-works-who-s-building-it-and-why-it-matters-now

Proof of Personhood: What it is and why it's needed. World. (2023, February 21). https://world.org/blog/world/proof-of-personhood-what-it-is-why-its-needed

Siddarth, D., Ivliev, S., Siri, S., & Berman, P. (2020, October 13). *Who watches the watchmen? A review of subjective approaches for sybil-resistance in proof of personhood protocols*. arXiv.org. https://arxiv.org/abs/2008.05300

Simons, T. (2023, April 23). *Trends in synthetic identity fraud*. Thomson Reuters. https://legal.thomsonreuters.com/en/insights/articles/trends-in-synthetic-identity-fraud

Social Security Administration Research, Statistics, and Policy Analysis. Social Security Administration. (2024). https://www.ssa.gov/policy/docs/chartbooks/fast_facts/2025/fast_facts25.html

Social Security Administration's Role in Combatting Identity Fraud. Office of the Inspector General. (2023, May 24). https://oig.ssa.gov/congressional-testimony/2023-05-25-social-security-administration%E2%80%99s-role-in-combatting-identity-fraud/

SSDI fraud update in 2024 | newlin disability. Newlin Disability. (2024, January 24). https://newlindisability.com/blog/ssdi-fraud-update/

White papers 2024 examining authentication in the deepfake era. ISACA. (2024, July 29). https://www.isaca.org/resources/white-papers/2024/examining-authentication-in-the-deepfake-era

Yamagishi, Junichi, et al. "ASVSPOOF 2021: Accelerating Progress in Spoofed and Deepfake Speech Detection." *arXiv.Org*, 1 Sept. 2021, arxiv.org/abs/2109.00537.