EMERGING FRAUD THREATS AND THE EVOLVING FRAUD LANDSCAPE

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

JULY 15, 2026

Serial No. 119–70

Printed for the use of the Committee on Oversight and Government Reform

Available on: *govinfo.gov, oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

64–225 PDF WASHINGTON : 2026

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, *Chairman*

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
ELIJAH CRANE, Arizona
BRIAN JACK, Georgia
JOHN MCGUIRE, Virginia
BRANDON GILL, Texas
RICHARD MCCORMICK, Georgia

ROBERT GARCIA, California, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
MAXWELL FROST, Florida
GREG CASAR, Texas
JASMINE CROCKETT, Texas
EMILY RANDALL, Washington
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona
WESLEY BELL, Missouri
LATEEFAH SIMON, California
DAVE MIN, California
JAMES WALKINSHAW, Virginia
CHRISTIAN MENEFEE, Texas
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JAMES RUST, Deputy Staff Director
RYAN GIACHETTI, Chief Counsel
JENNIFER KAMARA, Director of Strategic Initiatives
HANNAH CATHEY, Counsel
BILL WOMACK, Senior Advisor
MALLORY COGAR, Director of Operations and Chief Clerk
CONTACT NUMBER: 202–225–5074

ROBERT EDMONSON, Minority Staff Director
CONTACT NUMBER: 202–225–5051

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

PETE SESSIONS, Texas, *Chairman*

VIRGINIA FOXX, North Carolina
GARY PALMER, Alabama
TIM BURCHETT, Tennessee
BRIAN JACK, Georgia
BRANDON GILL, Texas

KWEISI MFUME, Maryland, *Ranking Member*
ELEANOR HOLMES NORTON, District of Columbia
MAXWELL FROST, Florida
EMILY RANDALL, Washington

C O N T E N T S

OPENING STATEMENTS

WITNESSES

Written opening statements and bios are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

The documents listed above are available at: docs.house.gov.

ADDITIONAL DOCUMENTS

These documents were submitted after the hearing, and may be available upon request.

EMERGING FRAUD THREATS AND THE EVOLVING FRAUD LANDSCAPE

WEDNESDAY, JULY 15, 2026

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:03 p.m., Room 2154, Rayburn House Office Building, Hon. Pete Sessions, [Chairman of the Subcommittee] presiding.

Present: Representatives Sessions, Foxx, Palmer, Jack, Mfume, Norton, Frost, and Randall.

Also present: Representative Walkinshaw.

OPENING STATEMENT OF CHAIRMAN PETE SESSIONS REPRESENTATIVE FROM TEXAS

Mr. SESSIONS. Good afternoon, and welcome to today's hearing on emerging threats and the evolving fraud landscape here in the United States of America. Over the years, the Government Operations Subcommittee, on a bipartisan basis, has held several hearings addressing the issue of fraud, addressing the things that the U.S. Government faces, as well as the American people. And each time we have been talking about fraud, how to identify it and how to prevent it. In our discussions, we have highlighted the importance of government agencies focusing on preventing fraud before it happens. And, as we have heard countless times before, once the money has gone out the door, it is hard to get back.

This remains a very important issue in this Subcommittee, to both the young Ranking Member and myself in this Subcommittee, is very important. But one critical element missing from our many conversations is what sort of fraud are we trying to prevent? How does it really work? What really are we doing about it? And where do we need to focus our attention to make sure that we are going to address this properly?

In our past discussions, we have referenced the fraudsters in a dark room stealing Aunt Sally's Social Security number. We have highlighted the risk posed by foreign actors applying to multiple disaster relief programs. We have discussed elaborate fraud rings that exploit loopholes in benefit programs in order to receive payment for services that they should not have received, but perhaps got the money.

But fraud threats are changing, and they are rapidly advancing. Identifying fraud threats specifically are booming as fraudulent actors become smarter and gain access to tools intended to make our life easier and their life easier through AI. This gives them more power. It is up to us to catch up. It is up to us to find it and to find a way that we are going to corner the market on our side of the agenda.

Government programs rely on identity verification to confirm that the individual applying for benefits and services are who they say they are. However, we have seen over the years the platforms used for these verifications have failed to meet the expectations.

In March 2023, this Subcommittee held a hearing focused on *Login.gov*. And the troubling findings from the General Services Administration's Inspector General report that was released that month told us point-blank we have a problem. In short, GSA misled government clients about the extent to which *Login.gov* met certain technical standards and expressly what they said it would do. These standards were the backbone of what was needed to ensure that an identity verification platform could prevent fraud, protect the taxpayer, and give the government the necessary information that it would need to know who they were speaking to and what that person might be eligible for, for benefits.

Over the years, many changes have been made to *Login.gov*, and Federal agencies have explored other public- and private-sector solutions for digital identification verification. As we are moving to a more digital environment where individuals may no longer be asked to present a physical ID card, we need to better understand what threats there are and what the fraud landscape looks like.

Today's fraud landscape looks different than the one that existed when we started this investigation, and it is rapidly evolving even today. Fraudsters from literally anywhere in the world can now create hundreds or thousands of synthetic identities and apply for many different government benefit programs simultaneously. It is no longer they could; they are. Bad actors are able to develop the use of deep fakes, mimicking the likeness of an individual to circumvent the safeguards that have been put in place to protect the taxpayer.

Bad actors have made it their business to exploit vulnerabilities in government programs. It is necessary that we understand that they have been successful, and we need to make sure we are developing the tools that actually allow us to see the fraud before it occurs, not when it is out the door. Identity verification has long been a one-time check at the beginning of an application process, but considering the rapid evolution of identity fraud, we should start thinking about validating and constantly validating identity as it moves forward.

Fraud should not be considered the cost of doing business because it means that someone is not getting the benefit that they were eligible for. And if there is one overriding principle that this Subcommittee, all of our Members agree on, it is that the people who we have intended the benefits to go to, they should be the ones that get it. And any diminishment of that is considered a failure on our part also.

In January of this year, I introduced bipartisan legislation to combat identity fraud and theft. The Stop Identity Fraud and Identity Theft Act aims to strengthen the Nation's digital identity verification infrastructure and protect individuals, businesses, and government programs from rising identity fraud and theft. I am hoping that this legislation is a step in the right direction. And after meeting with our panel members, I will tell you it is a step because we are going to learn more today in this rapidly evolving landscape that we call fraud, along with the verification systems that are available today.

We have a great panel of witnesses who can shed light on new identity fraud threats plaguing our systems, how the fraud landscape is evolving, and what the government should be doing and is doing to keep up with that. I look forward to a fruitful discussion.

And I want to personally thank our Ranking Member, Mr. Mfume, for his continued support. Those of you who are new to this Subcommittee will learn that both Mr. Mfume and I insist on making sure that we work well together, that we listen to each other, that we listen to all of our Members and allow them to fully participate, adding thoughts and ideas, but perhaps more importantly, to show up and listen and learn about the landscape that is directly in front of us.

Mr. Mfume is a very dear friend of mine. He is a man who has a distinguished service, not just to the U.S. Congress, but to the United States of America and to his district. And you will soon learn, those of you who are here, that we have many distinguished Members of this Subcommittee who are here because they believe in not only doing their job, but also helping us curb the appetite that fraudsters have to take advantage of our citizens.

With that said, I would like to now ask the gentleman if he would engage us with any opening statement he would like to make. The distinguished gentleman is recognized.

OPENING STATEMENT OF RANKING MEMBER KWEISI MFUME
REPRESENTATIVE FROM MARYLAND

Mr. MFUME. I want to thank you, Mr. Chairman, for your kind and clearly overly gracious set of remarks, for your friendship, for your stewardship of this Committee [sic], and for the ability for us on both sides of the aisle to really delve into detail on various issues, but none more important than this issue of fraud.

I know I speak for all of my colleagues on my side of the aisle when I say we welcome this hearing, as we did the previous one. We look forward to finding answers, quite frankly, and finding a way to get out of the situation that we are in with respect to the level and the significance of fraud within our government.

So, we are here today to talk about fraud, particularly emerging threats and solutions related to digital identity verification. Social Security numbers and paper cards made sense 90 years ago, long before the current age of computers and digital technology. Programs have matured, scammers have adopted them and found a way to get around them, and so the government must also, I think, adapt its service delivery and technology to prevent fraud and to better serve the American people.

That adaptation was exactly what the Federal Government had in mind many years ago when it came up with the idea and then later became the reality of something called *Login.gov*, which we are all familiar with, a single secure sign-in that works across agencies. Before *Login.gov*, each agency maintained its own identity verification. Good luck with that one. It was not just a headache for our constituents, it was also a costly overlap in functions and a critical cyber vulnerability.

While the GSA may have stumbled out of the gate with the initial release, we finally reached a point, I think, where agencies across all levels of government have a safe, secure, and verified gateway to government services that improves the customer service and helps our constituents across the services and the resources that their taxes pay for.

The turnaround in this program serves as an important example of bipartisan congressional oversight. Where once accusations of false promises dogged that program, *Login.gov* can now effectively serve the American people. We first learned, however, of the issues with *Login.gov* when the General Services Administration Inspector General published a report finding that several individuals at GSA had misled its agency customers that the system could do higher levels of identity verification than GSA itself. Those sort of things created problems.

Three years ago, we had a hearing exploring the issue and sent further follow-up letters, as the Chairman indicated, and briefings to ensure that GSA fixed the system that provided the service that they promised their agency clients. A year after our hearing, GSA announced it had fully implemented the National Institute of Standards and Technology's standard and had rolled it out to their agencies and to their partners. Today, *Login.gov* has over 100 million users across more than 50 agencies and 500 applications across Federal, state, and local government.

Now, that does not mean that the work to ensure digital identity verification across the entire Federal Government is finished. I look forward, like many of you, to hearing from our witnesses today about how we can effectively implement the next generation of *Login.gov* and identity management. However, we must carefully consider the difficulties and the pitfalls of the new technologies and not just assume that they do not have any.

Innovations like digital ID can better combat fraud and electronically safeguard identity, much more so than a 9-digit number on a piece of paper. Digital ID sounds great. I would not need to carry around a plastic license, just a smartphone if I am the average American citizen with cutting-edge technology to safeguard my personal information. The problem is, however, that that very phone provides a new vector of attack, and any computer is vulnerable to a cyber attack, as we know, regardless of its level of sophistication.

Digital ID can also limit access for people who have trouble using technology and even for people who cannot afford a smartphone. Sometimes, people just break their phones and cannot take time out of their busy day to immediately go and get a new one, so I do not think we can afford to lock people out of government or private services because they cannot access or afford a smartphone.

Anytime the government can revoke access to services, even for benevolent purposes, we must find a way to protect against abuse.

The Trump Administration's DOGE program, the Department of Government Efficiency, which many of us thought was the Department of Government Evil, used a key Social Security Administration identity database to mark thousands of living people as dead in order to exert financial hardship. A whistleblower recently said that he planned to expand this to millions of people. Now, do we really want to move to a system where the government can invalidate any ID it wants to just by sending an instruction to the phone that is in your pocket?

I can absolutely think of places where digital ID has valid uses for age verification and for fraud prevention, but every place that an American taps their phone to access services cannot be a "bread crumb to the track" or "bread crumb follow the track" process in their daily lives.

So, I am excited to have those of you who are here to discuss the new technologies to prevent fraud against the American taxpayer. We must also ensure that we keep an eye on the horizon to prevent any sort of mass surveillance and government surveillance that can literally decide if, in fact, we are considered live or dead.

So, I want to thank the Chairman again for keeping his commitment on this issue, for Members on both sides of the aisle that continue to plow through this. It has been a couple of years now. We are going to continue to do what we have to do until we cannot do it anymore. And I appreciate the opportunity to have all of you here and hear what you have to say on the record.

And Mr. Chairman, I yield back to you.

Mr. SESSIONS. The gentleman yields back his time. Thank you very much.

I would like to ask unanimous consent, if I can, to allow the distinguished gentleman, who has a meeting that he has to attend, to very quickly give some brief remarks.

I would like to yield time now to the distinguished gentleman, Chairman Gary Palmer. Chairman Palmer, you are recognized.

Mr. PALMER. Thank you, Mr. Chairman. Thank you for holding this hearing, and I would like to thank the Ranking Member for the bipartisanship that we have seen throughout this process in trying to address the fraud and also other issues related to improper payments.

This is an extremely important issue. I just came out of a meeting with Dr. Phillip Swagel, the Director of the Congressional Budget Office, and we estimate just the initial investigations into fraud that will have about $168 billion in savings. I want to make certain that people understand this is not just about the money. So much of this fraud mismanagement occurs in programs that are designed to help people who need help. And when we are losing that much money, we are being defrauded of that much money, those are funds that are not available for people who are truly in need. So, this is a huge issue for us, and it is not limited to domestic fraud. What we saw during the COVID pandemic, the programs at the Federal level were being defrauded by a massive network of foreign actors.

But we also have other issues, aside from the fraud. I think, one of the things that we found is that there is a tremendous need to modernize Federal data systems, bring them into the 21st century because a lot of the issues that we have with improper payments are directly related to antiquated data systems.

So, Mr. Chairman, I really hate that I am not going to be able to participate in this hearing. I think it is extremely important and would have benefited greatly from hearing the questions to our witnesses and their answers.

With that, Mr. Chairman, again, thank you for the privilege of being able to address the issue. I yield back.

Mr. SESSIONS. The gentleman yields back his time. Thank you very much.

Without objection, Congressman Walkinshaw of Virginia is waived onto the Subcommittee for the purpose of questioning the witnesses at today's Subcommittee hearing.

I now would like to move to welcome our witnesses who have taken their time today to be with us, and I am very delighted to say that I think that you will find and the Members will find their input very valuable to exactly the same things that the Chairman was talking about, and that is that we need to understand what is out there today. It is easy for us to think that we understand a lot, and we are going to learn a lot today.

So, I am pleased to welcome our witnesses. Mr. Jordan Burris is Vice President and the Head of Public Sector at Socure, where he partners with government leaders to develop and implement private-sector solutions for identity verification and fraud risk management.

Next, we have Marisol Cruz Cain, who is Director of Information Technology and Cybersecurity at the GAO. The Government Accounting [sic] Office has experts that provide not only expert testimony, but have an idea of the day-to-day activities that move across the government. She oversees Federal cybersecurity and privacy work. Her portfolio includes emerging technologies, the National Cybersecurity Strategy, and agency efforts to protect privacy, sensitive data, and critical computing infrastructure.

Next, we have David Maimon, and he is the Head of Fraud Insights at SentiLink, a company that combines technology and expertise to stop identity fraud at the application stage. He is also a professor in the Department of Criminal Justice and Criminology at Georgia State University, where he directs the evidence-based Cybersecurity Research Group.

Last, Mr. Jay Stanley is a senior policy analyst at the American Civil Liberties Union. His work focuses on technology-related privacy and civil liberties issues and that future and how it impacts public policy.

Thank you to each of you for joining us. I would now ask that each of you rise in pursuant to Committee Rule 9(g). The witnesses will each, as they stand, to take the—you can all stand please—to take the oath to the witnesses, and I would ask that you please raise your right hand.

I will read this and then let you affirm or choose as you would do.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you, God? That is a question.

Mr. BURRIS. I do.

Ms. CRUZ CAIN. I do.

Mr. MAIMON. I do.

Mr. STANLEY. I do.

Mr. SESSIONS. Please let the record reflect that the witnesses have answered in the affirmative. Thank you very much. You may all take your seat.

I have had an opportunity to speak with each of you, hopefully, except Mr. Stanley. Mr. Stanley, I want you to know that I have advised the other witnesses here that we appreciate you being here as we do them, that I run the Committee [sic] hearings differently. I would like for you to be able to finish your sentence. I would like for you to be able to complete your thought. I would like for you to be able to thoughtfully respond and provide this Subcommittee with the things which you have come professionally to do to us.

At 5 minutes, I am not going to bang the gavel. You are here. You are a professional. We need to hear from you, and I try and give that same type of leverage to each of our Members. So, I am delighted. But with that said, if you do not take advantage of it, I will not either. We have an idea that we are trying to move our business and allow our Members an opportunity to come and do their business also.

So, we will now move forward with the feedback from our witnesses, and we will first move to the distinguished gentleman, Mr. Burris. Mr. Burris, you are recognized for 5 minutes.

STATEMENT OF MR. JORDAN BURRIS
VICE PRESIDENT AND HEAD OF PUBLIC SECTOR STRATEGY
SOCURE

Mr. BURRIS. Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, thank you for your leadership on this critical topic and for the opportunity to be back here to be part of the conversation.

For the last 15 years, I have worked on one question from inside and outside the government. How do we know with confidence that the person on the other side of a digital transaction is who they claim to be? Today, that question has become far more difficult to answer. And here is the blunt truth. The way the Federal Government verifies identity was designed for a threat that no longer exists. Every day, however, we defend that old model as though it still does and give fraud networks another opportunity to steal taxpayer dollars and undermine public trust.

GAO estimates Federal fraud losses at as high as $521 billion every year. Further, the pandemic exposed just how far our identity infrastructure has fallen behind. Those losses were a warning. Today, the gap has widened dramatically, and by the time we update the next set of estimates, it will be double or triple the size.

My name is Jordan Burris, and I lead the public sector business at Socure. Socure was founded on a simple premise. In a digital world, proving who someone is should be accurate, fast, and fair. Today, our AI native identity and fraud intelligence platform helps

more than 3,000 organizations globally, including over 150 public sector organizations, make trusted identity decisions. That broad view allows us to see how fraud evolves across the economy and increasingly targets the government.

Before joining Socure, I served as Chief of Staff in the White House Office of the Federal Chief Information Officer, helping shape Federal identity policy through the COVID response and the government's transition to zero trust after SolarWinds. Working inside the government and in the private sector has shown me just how rapidly this threat has evolved.

Some of the identity industry have begun calling this moment World War Fraud, and I understand why. We are no longer confronting isolated fraudsters. We are facing organized, increasingly sophisticated, transnational fraud rings using AI at industrial scale. One fraud ring we profiled created nearly 25,000 synthetic identities and launched more than 35,000 attacks in just 30 days.

The adversary has changed. Our Federal identity model, however, has not, and yet many in the government believe it will hold up to today or even tomorrow's fraud threat. For decades, the government has treated matching a name, date of birth, and Social Security number validated against government authoritative records as proof of identity. That approach is no longer sufficient. Further, fraud does not stop at enrollment, and identity verification cannot either. It must become a continuous discipline that evaluates risk throughout the lifecycle of an account.

From where I sit, identity should be considered critical infrastructure. Nearly every interaction Americans have with their government—benefits, tax administration, disaster relief, veteran services, and healthcare—depends on getting this decision right. Done correctly, better security means better access. It makes it easier to say yes to legitimate Americans and no to industrialized fraud rings.

This year, Socure supported the Department of Education in deploying real-time risk-based identity screening in the Free Application for Federal Student Aid (FAFSA) process, protecting more than $1 billion in taxpayer funds, while allowing over 92 percent of legitimate applicants to pass automatically. That is the model the government should continue pursuing. Prevention before payment, risk-based rather than one-size-fits-all, continuous rather than point-in-time, and outcomes rather than checklists.

To make this the Federal model, I would leave the Committee with five recommendations. First, measure outcomes, not compliance, requiring systems to prove that they can stop the changing fraud threat.

Second, make continuous identity verification the standard across the lifecycle of an account.

Third, expand secure data sharing where we know it works, through trusted resources like Do Not Pay and other cross-government solutions.

Fourth, reward fraud prevention instead of recovery, where agencies are incentivized to stop fraud before taxpayer dollars ever leave the Treasury.

And finally, treat identity verification as dynamic infrastructure that must be resourced to evolve continuously, not built once, certified once, and left in place for a decade.

To be clear, Congress does not need to prescribe a specific technology, but Congress can establish a new expectation. The technology exists, and the evidence is clear. Now, our policies and practices must catch up to the threat, so Americans can trust their government in the AI era.

Thank you, and I look forward to your questions.

Mr. SESSIONS. Mr. Burris, thank you very much.

We now move to the gentlewoman, Ms. Cain. Ms. Cain, you are recognized for 5 minutes.

STATEMENT OF MS. MARISOL CRUZ CAIN
DIRECTOR
INFORMATION TECHNOLOGY AND CYBERSECURITY
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. CRUZ CAIN. Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, thank you for inviting GAO to contribute to this important discussion on identity-related fraud threats and Federal efforts to improve identity verification processes.

As you know, Federal agencies use personally identifiable information to verify the identity of individuals who access accounts on government websites. An increase in sophisticated cyber-attacks has led to a greater risk of that Personally identifiable information (PII) being stolen and used to commit different types of fraud. Malicious actors can then use that information to fraudulently receive government benefits, commit tax- or wage-related fraud, or create new credit cards or take over people's accounts. These attacks can harm individuals, result in financial loss, or damage the reputation of Federal agencies and financial institutions.

Because of this, GAO has long emphasized the urgent need for the Federal Government to improve its ability to protect against these cyber-attacks. Today, I will focus on issues related to identity-related fraud threats. I will also discuss the recent actions that GSA has taken to improve *Login.gov*'s identity verification services and alignment with Federal guidelines.

Fraud has been a longstanding issue within the Federal Government. One particular type is identity-related fraud, which can include thieves opening new accounts in someone else's name or stealing PII to obtain government benefits. For example, we have reported that hundreds of billions of dollars were lost to the—in the pandemic to potentially fraudulent payments.

The harms caused by breaches of PII or identity theft can extend beyond tangible financial loss to include lost time, such as when those victims spend months or years even working to restore their identities. Additionally, there can be reputational harm or emotional distress.

To address these issues, GSA developed *Login.gov* as a means to verify users' identities who want to create an account to access Federal websites. Accordingly, GSA has a significant responsibility for protecting users' PII that they collect during that process. In 2024 and 2025, we reported on *Login.gov*'s process for identity

verification, its misalignment with Federal guidelines for identity verification, and fraud prevention measures.

In our reports, we identified several weaknesses in GSA's implementation of *Login.gov*, including that the system did not meet the requirements to verify a person at the ILA–2 level, and that was because the system never included a physical or biometric comparison to link a user to a specific real-life identity. As a result, we recommended that GSA take four actions to ensure that the PII is better protected and to lessen the risk of identity theft. To its credit, GSA has fully implemented three of those actions. Most importantly, they have completed their remote identity proofing pilot, ensuring that the system is compliant with National Institute of Standards and Technology (NIST)'s ILA–2 standards. However, GSA has not taken important steps to collaborate with agencies to address *Login.gov*'s technical challenges.

GSA has developed a roadmap that outlines planned and ongoing efforts to improve its system functionality. However, this action alone does not fully address all of the technical challenges that we identified in our report. For instance, agencies reported that they lacked visibility into authentications, that the system had a high failure rate, and also, it lacked fraud controls. GSA's roadmap did not contain efforts directly aimed at addressing these challenges. It is important for GSA to work with agencies to solve these issues, as doing so will help ensure that *Login.gov* delivers the functionality agencies need to effectively verify users' identities while also combating fraud threats.

In summary, identity-related fraud threats are pervasive and likely to continue to escalate. Protecting individuals' PII is critical, as the harms can be significant. GSA has taken several actions to improve *Login.gov*, but needs to continue to address fraud and technical challenges.

This concludes my remarks, and I look forward to answering any questions you may have. Thank you.

Mr. SESSIONS. Ms. Cruz, thank you very much.

Dr. Maimon, you are now recognized.

STATEMENT OF MR. DAVID MAIMON
HEAD OF FRAUD INSIGHTS
SENTILINK

Mr. MAIMON. Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, thank you so much for the opportunity to testify today.

I serve as Head of Fraud Insight at SentiLink and as a professor of criminal justice and criminology at Georgia State University. For nearly two decades, I have studied cybercrime by going where it happens, into darknet markets, telegram channels, and encrypted platforms where fraudsters buy, sell, and teach each other how to steal from government programs. I also go into the field myself, to the mail drops, virtual offices, and shell addresses these operations use to look legitimate. My testimony today is based on that first-hand work.

The central lesson from my research is this: Fraud against government programs is no longer a series of isolated schemes. It is a durable, specialized criminal infrastructure, and it moves. The

pandemic did not create this infrastructure, but it supercharged it. Criminals learned how to acquire stolen and synthetic identities, stand up shell companies, open bank accounts, and recruit money mules at scale. When pandemic relief programs ended, none of that capacity disappeared. It simply migrated.

Today, my team is tracking that same infrastructure inside Supplemental Nutrition Assistance Program (SNAP), Medicare, Medicaid, Federal student aid, tax refunds, and Small Business Administration (SBA)-backed loans. A few examples illustrate how. We are watching criminals combine stolen identities with AI-generated faces and deepfake video to defeat liveness checks at digital banks and tax preparers using nothing more exotic than face swapping software available to anyone. We are watching an Electronic Benefits Transfer (EBT) fraud market where one criminal steals card data, a separate paid service verifies the balance before the card is even used, and the third actor cashes it out. And my own field investigation of a Florida durable medical equipment company, whose office I found abandoned in Delray Beach, is now tied to a Department of Justice case alleging $3.76 billion in fraudulent Medicare and Medicaid claims.

Different programs, different agencies, same playbook—the same stolen identity, the same shell company, the same bank account, reused across systems that rarely talk to each other. Debt fragmentation is the vulnerability. Criminals exploit the seams between agencies precisely because our defenses are built program by program, while their infrastructure is built to move across all of them.

Given my time today, I want to leave the Subcommittee with four priorities. First, replace self-attestation with verified data wherever the risk is high. Too many programs still take applicants at their word on income, identity, or eligibility. That was the single biggest vulnerability exploited during the pandemic, and it remains one today.

Second, expand real-time cross-agency data matching. The same identity that files a fraudulent tax return can apply for a SNAP benefit the same week. Agencies that only compare notes and periodic bet runs weeks after the money is gone cannot see that pattern. They need to see it before disbursement, not after.

Third, strengthen prepayment screening and move toward risk-based disbursement. Built on the model of Treasury's Do Not Pay system, but expand its authority and its reach so that suspicious payments are held before they leave the government, rather than chased afterward through recovery audits that criminals have already outrun.

Fourth, give agencies the flexibility to adopt smarter tools and keep it current. Much of today's verification infrastructure and the policies behind them were built for an earlier threat. And procurement and rulemaking cycles that take years cannot keep pace with fraud tactics that shift in months or less. Agencies need standing authority to test and deploy technologies to meet the current threats, not just at the next scheduled audit. None of this requires slowing down help for legitimate applicants. It requires distinguishing them from fraud earlier, using signals criminals cannot easily fabricate.

The Federal Government already has some of the tools it needs, what is missing is the authority, the coordination, and the sustained investment to use those tools before the money moves, not after. Every dollar we protect from organized fraud is a dollar that stays available for the people Congress intended to help.

Thank you, and I look forward to your questions.

Mr. SESSIONS. Dr. Maimon, thank you very much.

Mr. Stanley, welcome. We are delighted that you are with us. The gentleman is recognized.

STATEMENT OF MR. JAY STANLEY (MINORITY WITNESS)
SENIOR POLICY ANALYST
AMERICAN CIVIL LIBERTIES UNION

Mr. STANLEY. Thank you so much. Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, thank you for inviting me to testify today, and thank you for your attention to the subject of digital identification, which I do not think has received the attention it deserves.

I hope to leave you with three overarching points today. First, a digital ID system would be a disaster for individual liberties if it is not done right. If any such system is to become standardized, it must be built with great care and awareness of big potential downsides. We have to ensure America does not become a checkpoint society and that digital IDs do not become virtual ankle monitors, something that tracks us, but we cannot turn off or escape.

Second, the digital ID system that is most likely to become dominant, mobile driver's licenses or MDLs issued by the states, is not being done right. Driver's licenses are already in most Americans' wallets and are by far the most likely form of digital ID to become standard. *Login.gov* itself is moving toward relying on them.

Third, there are much better alternatives if we just do it right.

So, let me start by explaining my first two points, that digital IDs have the potential to be a disaster if they are not done right, and that they are not being done right today. One big problem is that once this infrastructure is built, we start getting identity requests from every direction. Want to enter a 7-Eleven? Scan your ID. Want to buy a cup of coffee, park your car? Tap here, please. Want to watch a video, log into social media, look at a news site, shopping site? Click here to send us your driver's license.

There is already far too much tracking that takes place online, and polls show Americans are very uncomfortable with it. But there has been a steady pushback, and that tracking has been getting harder for companies in some ways. A digital ID could lock it down and make it inescapable. You cannot just run to the Department of Motor Vehicles (DMV) and get a new identity the way you can get a new username and password.

Those pushing MDLs in the states have done nothing to counter this easily predictable side effect. We may create a digital ID to solve government fraud or identity theft or other problems, but there is a horde of others waiting in the shadows who will instantly pounce on this infrastructure to use it for their own purposes once it is created. The result will be a checkpoint society of constant ID proofing. With a digital ID that will be really easy. Just tap, click, or scan.

And a digital ID system, if not built carefully, could send a report back to the government every time you show your ID, a record of every beer purchase, bank, and doctor's office visit, and online, every website you visit. This is called "phone home." This capability was built into the MDL standard as an option.

There is also the issue of accessibility. If digital IDs become mandatory, either legally or as a practical matter, that would harm the surprisingly large number of people who do not have a smartphone, about one in ten people in the United States according to studies, including over 1/5 of people over age 65. Some may lack the resources to afford one; others, the technological literacy to use them. That is why offline options for doing business are vital to protect. If we do not make sure that digital IDs are an empowering option for people rather than an imprisoning requirement, then people without smartphones will be shut out of many necessary functions of life and often benefits that they sorely need. So, these are easily foreseeable, predictable consequences of a digital ID.

But that brings me to my third point. If a digital ID is to be created, there are alternative paths that would prevent many of these harms. In terms of alternatives, I have two quick points to make before I stop.

First, the field of privacy-enhancing cryptography is advancing fast and already can do amazing things that allow us to have our cake and eat it too when it comes to privacy and security. One example is privacy-enhancing technology called zero-knowledge proofs. Using that kind of tech, digital IDs can let me prove I am over 21 without sharing my date of birth or my identity. And it can do that in a way that if I prove my age multiple times to the same seller, they do not even know that I am the same person. That is the kind of thing that is needed to stop IDs from being this kind of ankle bracelet tracker.

But that kind of technology is useless if we do not bother to build it in, and it has not been built into the MDL standard. If a system can reduce fraud and provide other benefits without enabling tracking, why would we build one that does enable tracking? There are other key protections we can build. On our website, we have outlined 12 key protections that we think are necessary in a digital ID system. There is more about that in my written testimony.

And then, second, there are some states that are moving in the right direction here. Some, like New Jersey and Illinois, have put some important protections in place into their digital ID-enabling legislation. And the State of Utah is the most notable. It has set out a separate path, which they call State Endorsed Digital Identity, or SEDI, that is emerging as a far more privacy-protective alternative to the MDLs that many states have adopted. Some other states are starting to work with Utah to join in that effort and build that alternative path.

The bottom line is if we build a digital ID system, it must be done right. We urge Congress to ensure that it is. American freedom is the top priority.

Thank you very much, and I look forward to your questions.

Mr. SESSIONS. Mr. Stanley, thank you very much. I appreciate each of the witnesses being here.

I would like to move first to the distinguished gentleman, Mr. Jack, for his questions. The gentleman is recognized.

Mr. JACK. Thank you very much, Mr. Chairman.

And I appreciate your testimony this morning, Mr. Burris. My first question is for you. The public increasingly relies on the internet to access government services, and I am just curious, from your perspective, what fraud threats might my constituents be facing that they are not even aware of yet?

Mr. BURRIS. Representative, thank you for the question. When it comes to the fraud threats and the way that they are evolving across the landscape, every single interaction, every single time that an individual is engaging both with their government and in their commercial life, there is the chance, the opportunity, that an adversary could be attempting to pose as them, could be attempting to enroll in an account. We see this across financial services where we work. We see this across various aspects of the gig economy where we work, and then, of course, with government organizations.

The reality here is that all of the information, all the PII that exists for many folks within this room has been stolen by the adversary, and they are using that to attempt to become them, and therefore, that they can access what would be either their bank accounts and help move money all across the economy.

Mr. JACK. You know, I have heard folks mention anecdotally that now with artificial intelligence, people are trying to impersonate, you know, a loved one by virtue of maybe their voice or their mannerisms, what have you, and using some of that information that may have been stolen. Have you seen that, and could you elaborate on that for us?

Mr. BURRIS. Yes, absolutely. We are in a, what I would consider, a national crisis from where I have said, I have highlighted and our team has highlighted—Socure—for a number of years now that the moment that we are in is unlike any other in the sense that AI is being used as an accelerator for what attacks that typically would take weeks to occur. And further, it is also becoming more cost-effective for the adversary to launch those attacks. So, these attacks could be everything from launching deepfakes, things where we have seen an 8,000 percent increase year over year.

This can also be in terms of the velocity by which attacks are happening. This means the speed by which they are occurring. And in these instances, these moments, we are seeing things that—where attacks used to take weeks in order to be conducted, they have been broken down to under 48 hours. And this would mean that an adversary has launched an attack where they have stolen my information or yours, or even worse, fabricated an identity, attempted to open an account and/or move money, take over an account that may have existed because they went through a call center and were pretending to be you using your voice or something that was cloned, an image of yours, a biometric, et cetera, and they have used all these patterns. And if, like, for, say, they were blocked in some way, shape, or form, they then just adapt and iterate, and the cycle continues all over again.

Mr. JACK. Thank you very much.

Dr. Maimon, do I understand, are you a professor at Georgia State University? So, I wanted to acknowledge, first and foremost, both my mother and father went to Georgia State University. I represent many people who have degrees from Georgia State University, and I also host Panthers in the district from time to time, so bringing students up here.

So, I am curious, to build off that last question, you obviously understand, you know, criminology, you are a professor of it. Help us understand, are most of these threats coming from inside our country, or are we starting to see foreign adversaries exploit some of this data to, you know, fraudulently impact some of our constituents?

Mr. MAIMON. Thank you so much for the question, really appreciate it. A lot is coming from abroad. We have a lot going on internally as well. It really depends on the type of fraud we are looking at. In the context of the type of fraud you just mentioned, with folks engaging in online romance fraud, we are seeing a lot coming from places like South Asia. A lot is moving right now to Africa. In some of the online fraud markets that I infiltrate, I spend a lot of time sort of trying to infiltrate Yahoo Boys channels, as well as Sakawa Boys channels, where I actually see them using those deepfakes to swap faces while engaging with some of the victims here in the United States.

It is heartbreaking to see the level of conversations that these guys are able to get with those targets, and it is also heartbreaking to see the different modus operandi and different types of buckets that those criminals are engaging. I can tell you that, as of this morning, we are seeing more and more Yahoo Boys and Sakawa Boys targeting our 401(k)s, victims' 401(k)s. So, you know, we are seeing them convincing targets to borrow against the 401(k)s, as well as hand over control completely on the 401(k) accounts. So, this is what we are up against. We are seeing those deepfakes being used to swap faces, lure targets to give away access to the 401(k) accounts, and then, unfortunately, victims funnel the money to bank accounts that the criminals create, along with the targets, and then the money leaves the country.

So, it depends on the type of fraud. The type of fraud that you are referring to definitely comes more from abroad.

Mr. JACK. I appreciate all of your testimony today, and, Mr. Chairman, I am grateful you convened this hearing. I have learned a lot already in just this interchange, so thank you very much. Mr. Chairman, I yield the remainder of my time.

Mr. SESSIONS. The gentleman yields back his time. Thank you very much.

The distinguished gentleman, Mr. Mfume, you are now recognized.

Mr. MFUME. Thank you, Mr. Chairman.

Mr. Burris, I want to start with you because something you said struck me, and it might be the basis of why we are here and why we want to come back this way again, and that was that you said, if I am paraphrasing you correctly, that we are spending years and millions of dollars preparing for a threat that does not continue to exist. Can you expand on that, please?

Mr. BURRIS. Absolutely. And in particular, the part of my testimony that I was highlighting was the fact that much of how the Federal Government has thought about its standards for how to prevent or protect digital identity—and to be very clear, digital identity is the makeup of how we present ourselves in cyberspace, right? Much of how the government has designed that standard today effectively was worked about a decade ago. And so, if we are looking at today's fraud threat, how it has evolved, how the adversary moves, it no longer can keep pace with what we are seeing today.

So much so one of the efforts that, you know, our company led was, as we were engaging with NIST as part of their most recent update to the standard, was highlighting that fraud should become an underpinning of part of what we evaluate in digital identity and when it is established. Not because we want it to be harder for people to prove who they are, but because the alternative is that we are leaving a floodgate open for nation-states to launch their attacks. And from where we see it today, you know, there are over 7,500 fraud rings that are operating in their own different ways to attempt to attack what would be government services or even the commercial sector.

Mr. MFUME. And Mr. Burris, as artificial intelligence advances at an alarming rate, what does the government, and in particular, what does *Login.gov* need to do to stay ahead of those scammers and to be able to identify them as we move forward?

Mr. BURRIS. It all starts with admitting that there is a problem, so we are going to begin there and say that this is a crisis moment for where we are in. I think it is important that we understand that, as the Federal Government, we need to basically embrace and understand that we need to use AI to fight AI at this point. The adversary does not care about how anything is constructed, they do not care about our norms, they do not care about rules and regulations, they do not care about the ages of those who they are engaging with or their political affiliation. What they are attempting to do is to take money and resources to disrupt what would be the status, the norms, that we hold dear. And what we need to do is engage aggressively to basically put in place the types of controls and measures, many of which have been adopted in other sectors for years, in order to help prevent against this threat.

For *Login.gov* in particular, I would say, and, you know, full disclosure, again, we are one of the vendors that are now have been added in order to power what *Login.gov* is doing. They are taking this threat absolutely seriously. In this day and age, another fraud team has engaged diligently to understand what needs to evolve with the program.

Mr. MFUME. And Ms. Cruz Cain, you mentioned at some point in your testimony, I am trying to get back to it here, where GSA implemented four or five recommendations. What was the fifth recommendation? Is that still standing?

Ms. CRUZ CAIN. We made four. They implemented three. And the last one was the agencies, the 24 Chief Financial Officers (CFO) Act agencies that we talked to, had technical challenges with *Login.gov*. So, as users, they were not necessarily able to use with ease, and they had some issues with the platform, such as they

would like to know when the users are verified and authenticated, why they were not. So, if they fail, the person just says, hey, I failed. They have no way of knowing why they failed, how they can remedy that, so then you just do not have access to your government account so you cannot get your benefit. You have no recourse of knowing how that happens. So, either you just have to try again, or you have to go to the post office. That was one of the issues.

Another issue is, at the time, they had a high failure rate, so they were just getting problems of even logging into the system or being able to use it. And at that time, they were not having such strong fraud controls. And again, to their credit, they have been taking the issue very seriously and partnering with new technologies and new companies to enhance their fraud controls. But they need to partner with the users to make sure that they are also helping them with the issues that they are having with *Login.gov* because if the users cannot use it—the technologies can be great, but if your users are still having issues using the system, you are going to lose that user base.

Mr. MFUME. Thank you very much. Just one other quick question. Mr. Stanley, I appreciated your description of a digital ankle bracelet or ankle monitor, and you referenced driver IDs. Are they the most vulnerable?

Mr. STANLEY. I think that, in many ways, cryptographically secured——

Mr. MFUME. Driver's licenses.

Mr. STANLEY [continuing]. Digital driver's licenses——

Mr. MFUME. Are they less vulnerable?

Mr. STANLEY [continuing]. Are less vulnerable, probably, than many other techniques for validating identity. Mr. Burris talked about use AI to fight AI. There are many technologists who say that that is a losing battle, and that you will never—it will always be a constant arms race because any AI that can be used to identify who is real versus who is not, that same AI can be used to fake somebody who is not real. And so that is why a lot of people in the technology world are turning to cryptographically secured tokens or identities so that, basically, the DMV or other issuer takes the data in your driver's license, digitally signs it with encryption, with a secret key, and then publishes a public key, and a verifier can look at the public key, and if it matches, it could only have been signed by the DMV and not a single bit could have been changed.

And that is cryptography. And so, somebody can prove that the thing they have in their phone, the file they have in their phone, was issued by the DMV and signed by the DMV. And that is one of the reasons why we think that digital driver's licenses are poised to move to the forefront in online verification and why we worry about all the side effects of that kind of a system that I talked about.

Mr. MFUME. Thank you. Thank you very much.

I yield back, Mr. Chairman.

Mr. SESSIONS. The gentleman yields back his time.

Ms. Norton, you are now recognized.

Ms. NORTON. Thank you.

Digital identification and modernized technology systems can help verify identities and reduce fraudulent claims, but they should

not come at the expense or access to vital social safety net programs. Mr. Stanley, as more Federal, state, and local governments adopt digital identification systems, who risks getting left behind?

Mr. STANLEY. Yes, so exclusion is a big potential side effect of this kind of a system, and we will need to ensure that a digital identity is not mandatory, and we will need to pay the costs of ensuring that there are other options, lest we dial up the security dial too high and leave a lot of people who have genuine needs and are genuinely qualified for benefits being locked out.

We know, in addition to what I said, about 20 percent of people over age 65 and ten percent of Americans not having smartphones. Studies have found that people with disabilities are 20 percent less likely to have smartphones. People with incomes under $30,000 a year, 25 percent do not have smartphones. Thirty percent of rural Americans lack fixed broadband and good internet access, and many people with low incomes are on limited data plans.

And so, basically, we need to ensure that we never assume. And a lot of these things will improve over time. Some of these studies are a few years old and probably are out of date already, but we are never going to get to the point and we should never make policy based on an assumption of 100 percent adoption of technology because there will always be people who cannot or will not or simply do not want to and should have the freedom not to use all these advanced technological systems. So, I hope that answers your question, Congresswoman Norton.

Ms. NORTON. Mr. Stanley, which populations are most likely not own smartphones?

Mr. STANLEY. Sorry, the populations most likely not to own smartphones?

Ms. NORTON. Yes.

Mr. STANLEY. Yes, it is again, older Americans and low-income Americans, disabled Americans. Low-income Americans, of course, are disproportionately people of color, and so I think those are the populations that would be most affected. People who are—often already face a lot of marginalization in life may find themselves further locked out of paths toward fully living in our society.

Ms. NORTON. Well, Mr. Stanley, given the increased adoption of digital identification, are people without smartphones at risk of reduced access to government services?

Mr. STANLEY. Well, yes. What we see is that something—a technology like a digital ID tends to move over time from being an option that empowers people, to being expected, to becoming normalized, and then people who do not have it end up as freaks and edge cases that just are not accounted for by the systems that run our governments, our benefits, and many private-sector goods as well. And so, because often it is expensive to maintain offline, real-world options for people, but it is important that a digital identity system do remain an option. There are post offices in every town in America where people can do things in person. There are other offline ways of doing things, and we need to make a conscious policy decision to protect those ways, those alternatives, to protect American freedom and to protect people who are vulnerable and need the benefits that they are qualified for.

Ms. NORTON. Even for those who do own smartphones, a lost, stolen, damaged, or nonfunctioning device could temporarily prevent them from accessing the programs they rely on. While we should embrace new technology to minimize fraud, we must ensure all Americans have access to programs.

I yield back.

Mr. SESSIONS. The gentlewoman yields back her time. Thank you very much.

I now recognize myself for a UC, unanimous consent request. I would like to enter into the record two letters that have been provided to the Committee, both Mr. Mfume and myself. The first is a letter from the Better Identity Coalition. They highlight how digital identity credentials like mobile driver's licenses and investments in digital identity infrastructure could help address this emerging fraud threat that we are talking about.

Second, the second letter is from the Defense Credit Union Council. It reinforces how critical it is to protect the Nation's military and veteran communities against scammers who specifically look to exploit vulnerabilities created by their life in the military and to take advantage of that. So, without objection, so ordered.

Thank you very much.

It is intuitively obvious to each of us that my side, the Republican side, the Majority side, does not have many Members here. We are in the middle of receiving a briefing on the conflict in the Middle East at this time by the Administration, and so I have chosen not to cancel this hearing but rather to stay myself, and so I may take the place of some of my Members, so I would yield myself my time right now.

Mr. Stanley, thank you for being here. Mr. Stanley, I would like to ask a question that really came to me today, and I find very interesting, not only your comments, that I find common sense and I find myself—I would have to struggle with myself to disagree with you. But it brought up one issue, and that is we generally see fraud as an overwhelming factor that we need to defeat, that when fraud is involved—and fraud could be something that then becomes tangible where it has been established, necessarily established as opposed to questioned to establish whether it is fraud.

Where fraud is involved, are there limitations on behalf of the government to satisfy the requirement of protecting themselves? And the for-instance I would like to give is, at an airport that I go to every week called Reagan Airport, there is a sign from the government that says if you are in this area, you are subject completely to search and seizure. In other words, we can do, by and large within some balance, what we want to do, to ask you, to demand you to comply with our orders and those things. Is there a point at which we should be careful once we know fraud is involved? And I can give you probably several instances, but I want to ask that question to you.

Mr. STANLEY. Mr. Chairman, I am not sure I totally understand the question. My apologies.

Mr. SESSIONS. Okay. So, I will try and help it out. When we think that we have established the standard of fraud by a government agency, and they then are saying, we are dealing with fraud, is there a limit to how far they can go within reason but to estab-

lish something? For instance, could they pick up the phone and call a bank, "know your customer," and a bank would have an idea that they are involved.

And we are trying to move a lot of these issues to professionals in law enforcement and professional otherwise. Could they call a bank and say, can you please tell me, I have got a customer that lives at 1515 Smith Avenue, and this is their name, and they tell me they are 68 years old, and they told me that they do this, and this, and this. Is that okay? Because they have established fraud, and they are trying to then run it down. What are the limits? What is the expectation that you have?

Because you have mentioned civil liberties a few times, and I respect that, but we are talking about fraud, and we are talking about how would you expect the government—are there parameters? The government can only go so far? Are we going to give the criminals that upper hand? So, that is the question, sir.

Mr. STANLEY. Okay. Yes. So, if you are talking about investigating fraud that you have evidence it has already happened, I think that it would become a criminal investigation like any other, and that has been—that is subject to the Constitution, the limits of the Constitution, you know, presumption of innocence, and the Fourth Amendment to the Constitution prohibiting unreasonable searches and seizures, and other provisions of the Constitution that have been well litigated over the years. So, I would think that a professional law enforcement officer would know what those limits are in many ways. And whether——

Mr. SESSIONS. Have you had a chance, Mr. Stanley, to look at the piece of legislation that was passed by this Committee a few weeks ago that is waiting for floor arrival that would take these options and move them to the Inspector General (IG) in the Treasury Department in a specialized unit that are law enforcement-type people? Have you looked at that?

Mr. STANLEY. I confess that I have not. I would be happy to and get back to the Committee with our views on it.

Mr. SESSIONS. If you could do that, I am interested in your feedback because we are trying to say that we believe once a standard of fraud has been established, that there needs to be specialized, sure, but the ability that investigators have to go and vet this, we just have to find a way. Is it truthful? How widespread is this? And how are we going to handle this?

Okay. I am going to ask you another question. Got 5 seconds left, but we are kind of being a little careful. We are not as tight on this. The second one is, is there a limitation on someone if they are presently on Social Security, they have taken out a loan, SBA, something where they are in the government system and we find some instances where there might be questions that arise? And I know once again, you are very careful, and I agree with that, within the law, within the Bill of Rights, within the Constitution, within all the things that we could establish. Is it fair game to go back and run people back through if they think there is something that might be amiss through this organization, even though a person has been on government benefits? Because, you see, we think that a lot of people that presently are receiving government benefits might not be exactly as we thought they were. Is that fair game?

Mr. STANLEY. I think it is with some cautions. I think if a government agency sees signs of fraud, there is no reason why it should not——

Mr. SESSIONS. Right, that has to be established.

Mr. STANLEY. There are cautions, especially if you are looking at, for example, using AI algorithms in order to do that, that may have been trained on sets of preexisting data that contain biases. There was a man—there was an *NBC* report, which I could share with the Committee about it, who paid his credit card off every month in full, and he got a letter from his credit card and they said we are reducing your credit limit. And he said, why, I pay off in full? They said because we have found that the other store—other customers at some of the stores you shop at have been bad credit. And I think that that strikes most people as just unfair and guilt by association.

Mr. SESSIONS. That would be a smell test.

Mr. STANLEY. But I think that a lot of AI algorithms do basically the same thing in a hidden way.

Mr. SESSIONS. How about if AI discovered that there are 74 people at your home address that receive benefits because AI discovered it, and we think that you might be one of them, and we would like to do some sort of a review about this? Is that fair game?

Mr. STANLEY. I think that there are good uses of AI and that flagging that kind of anomaly, as long as there is human review, might make sense. But, for example—for examples like that, there are other examples where we see, unfortunately, government agencies not building in the checks and balances, the due process, and using AI not only to figure out who it thinks is suspicion, but then to take actions against people that they have trouble, you know, getting due process and fighting back. We have seen, for example, in states, people losing their disability benefits based on algorithms.

Mr. SESSIONS. Okay. So, let me give you that. It would then at some point require human intervention to review data to then make some decision as opposed to a computer automatically assuming something.

Mr. STANLEY. I think that is right. The only other caveat I would add is that some of the fraud prevention techniques are based on gathering an enormous amount of intrusive data about individuals.

Mr. SESSIONS. We spoke about this, but you had indicated earlier, without human intervention, that meant that someone else, a computer or an AI modeling, decided they could send you a letter and cutoff your benefits. I am saying that we could use these to then go to a human who is trained, who does have this professional experience, who would be able to apply it, and then would be able to use some rational basis. Okay. So, you would agree with that?

Mr. STANLEY. Yes, but what I am saying is that, for example, there are industries that use unethical apps on people's smartphones to track their location without their knowledge or permission. I am sure that many people in this room are being tracked by these companies without knowing, and that some of that data can be fed into these algorithms for deciding who is suspicious and a lot of other very privacy-invading data. So, if the algorithm you

are talking about is based on that kind of very intrusive privacy-invading data sources, we would have a problem with that.

Mr. SESSIONS. Okay. Well, I could bring up lots of examples. I am not going to. I want to thank you. I think this is an important question. That is why you are here today.

We would now like to move to the distinguished gentleman from Florida, Mr. Frost. Mr. Frost, I yield back my time. We now move to you. The gentleman is recognized.

Mr. FROST. Yes, thank you so much.

You know, part of my concern as it relates to digital ID becoming mandatory is the risk of widespread data collection and exposing millions of Americans to harm, which is already an issue that this country seeped into many different ways, social media, online, and different things like that. Mr. Stanley, how could digital ID systems become a barrier for Americans trying to access services, benefits, or programs?

Mr. STANLEY. That could happen if, first of all, you are unable to get a digital identity system because you do not have a smartphone. There are also a lot of Americans who do not have access to—who do not have, currently have, any kind of driver's license or non-driver ID from DMVs, who—there are people whose birth certificates were burned in a fire in Tennessee in 1955 and do not have access to them.

It is a messy world out there, and I think that digital IDs seek to impose a sort of neatness and bureaucratic, you know, regimentation on it, on all of us. And so, in making policy, we have to make sure that people who do not have access to those things are not left out. So, you cannot get—there are people who cannot get a driver's license. There are people who, maybe they have a driver's license, but they will not be able to get a digital driver's license because of the things that we talked about in terms of not having access to the technology or the technological literacy to use it. There was one study that found that a very large proportion of people over 65, you know, were not able to install an app on a smartphone.

There could be situations where people's IDs are abusively revoked. You know, we have seen, there has been mentioned that the Trump Administration put some people in the Social Security dead file. We also saw in California, a Democratic candidate for Governor proposed that Federal agents who wear masks should have their driver's licenses stripped from them. And whatever you think of mask-wearing by Federal agents, which is a controversial issue, that is using an identity infrastructure for political purposes, which is something that we may see in the future left, right, or center, and so that could be a threat. And we have called for protections against people having their IDs yanked by abusive governors or the like. So, those are some of the ways in which people could find that they are left out of a digital identity infrastructure.

Mr. FROST. Part of my concern, too, is when we look at this Administration, we know they have empowered big tech companies like Palantir to create databases of Americans' personal data for government use. We know that during the, you know, DOGE era, similar things were done during that as well. This data collection could make it easier for private companies to abuse our data. I know some proponents will say, well, you know, this is mainly for

government use, but we know it is not only for government use. And that is part of my concern with this. There is just so much collaboration between private companies, data sharing.

How should we legislate on balancing the convenience and the real dangers of digital ID? Which also will lead to losing anonymity online, which is something else I am concerned about as well.

Mr. STANLEY. Yes, we have a piece on our site that outlines 12 protections that we call for that we think state legislatures should enact that govern any, you know, mobile driver's license or digital ID that is created in their state. I will not go through them all, but they include such things as protecting people against incessant demands from every corridor. If you want to do business with us or come in our candy store, you have to tap your ID and give us your driver's license to get in.

Mr. FROST. Yes, this is part of my concern, too, that making it easier to prove who you are will lead to more services, companies asking you to do so for every service that is not expected of you right now.

Mr. STANLEY. Yes, it is an excellent point because one of the things that, you know, if you are a website and it is really, really hard to prove your identity online, you have to take a photo of your ID, you have to send it in, you have to get a video, you have to do proof of liveness, all this stuff. You are not going to ask your visitors, your users to do that unless you really need to, so that imposes a limit. But by getting rid of all the friction of proving who you are online, you get a pop-up like the privacy pop-ups we get today, click here to send us your digital ID. It will not only become easier for me to share my digital ID, that means that it makes it much easier for them to ask me to or demand that I do so.

And that is one of the big things we have—and that is one of the protections that policymakers can make, which is to say, these are super IDs, they are cryptographically locked down, DMV vetted, everything like that. This is, you know, and that you should not be forced to use a super ID to prove your identity unless it is legally required, we have called for, maybe in certain other specific situations.

But people are going to need protection against this absolute, you know, waterfall of demands that we can easily anticipate are going to happen once this is created. And then other protections like privacy protections to make sure that the wallet holders do not, are not spying on everybody, and that, you know, that these cryptographical things that I talked about are built in to protect privacy so that, you know, you can prove things about yourself without having to, you know, create a lifelong relationship with somebody by identifying yourself to them.

Mr. FROST. How can we—and I know we are over, if you can indulge me, Mr. Chair. My last question is how can digital ID lead to complete loss of anonymity online?

Mr. STANLEY. Yes, so, I mean, the websites are going to want everybody to identify themselves all the time. They are going to want to do it because their ads will be worth more if they know who you are, and they can plug in you—the data they have about you to other data they get. They are going to want to do it to make sure that you are of age so they can market to you under Children's On-

line Privacy Protection Rule (COPPA), which is, you know, you cannot market to people under 13. Identity verification, which has become a big controversial issue. And bots, a lot of sites are having problems with AI impersonating humans, and they are going to want to know that you are a human for various reasons, and so there is going to be a lot of pressure for a lot of websites to start demanding this——

Mr. FROST. Yes.

Mr. STANLEY [continuing]. All the time.

Mr. FROST. And part of the concern, right, is the fact that this information can be weaponized against consumers, working people, who are looking to purchase things online and have that information leveraged against them when they are making decisions on what they want to buy and how much those items cost, correct?

Mr. STANLEY. Yes, surveillance pricing, where stores get a bunch of data about their customers, and then they charge you based on what they know about you and how much they think you will pay and whether you are desperate and so forth. That has become a very controversial issue, and states, you know, regulation of surveillance pricing has been attracting support in the state legislatures from both left and right. And digital IDs will make that much easier because if you know they are going to charge—if the store is going to charge you more—like, let us say that the airline happens to know that you have just lost a close loved one and you have to fly, they can up your price.

Mr. FROST. Yes.

Mr. STANLEY. And so, you are going to want to see what the price is without them knowing who you are, right? But they are going to want to know who you are, and there will be this arms race. And a digital ID would sort of end that arms race——

Mr. FROST. Yes.

Mr. STANLEY [continuing]. And you cannot escape them knowing who you are——

Mr. FROST. Yes.

Mr. STANLEY [continuing]. If it is done badly.

Mr. FROST. Yes, I appreciate it. Thank you for indulging me, Mr. Chair. I just think, you know, I am not a Luddite, and I just think these conversations are important because it shows how much care and intentionality needs to be put into this.

Oftentimes, we are very excited about something, we move quickly on it without thinking the next 10, 20 years into the future, and then it is an emergency for another generation to handle. I think we have to have these conversations now and legislate accordingly.

Thank you. I yield back.

Mr. SESSIONS. The gentleman yields back his time. Thank you very much.

The gentlewoman from Washington is now recognized.

Ms. RANDALL. Thank you so much, Mr. Chair, and thank you to our panelists for joining us.

You know, *Login.gov* gives every American a one-stop portal so they can use a single username and password to log in across a variety of Federal programs. Sounds like a benefit and a, you know, customer service improvement. This is a portal that state and local

governments can use as well, and it saves taxpayers time and money and generally makes life easier.

Mr. Burris, can you briefly describe how *Login.gov* has leveraged Socure's technology to help reduce identity fraud for government programs?

Mr. BURRIS. Absolutely. And I think a lot of this comes down to trust and basically leveraging what would be considered next-generation technologies to try to help balance. A lot of the conversation I have heard are around access and speed and confirming that the right people ultimately can access these services.

So *Login.gov* conducted a competitive procurement where they evaluated our technology against that of 17 others at the time, and they incorporated different components of our solutions, everything from solutions that we have around document verification, so confirming that it is a legitimate government-issued ID, and/or what would be facial biometric comparisons, so the idea is comparing it and confirming that it is actually the right person on the other end of the screen. They also incorporated what would be additional fraud models to their stack, things that they are incorporating such as identifying and understanding what is happening with the device a person may be using because it is all too often that the adversary would do something such as take a jailbroken device that is overseas and attempt to say that they are operating within New York or D.C. for that instance, also doing comparisons with things like the phone or the address of individuals using their email.

And then some of the flagship offerings that we have related to helping to paint a picture or prediction of whether or not it is someone who is engaging in what would be a pattern that is associated with identity theft and/or synthetic identity. And far too often, what we see in the industry is that kind of weaknesses in these technologies have led to this unfortunate conversation about folks who have been left out and forced down alternative paths. It has always been my belief that if someone is choosing to engage with a digital service in government, they should be able to do so, and the technology should adapt to meet them where they are. So, the addition of Socure's tools have enabled *Login.gov* to take strides toward being able to address that and make their service more accessible while simultaneously combating fraud.

Ms. RANDALL. Thank you so much. It is really great news that we are innovating in this way to provide access that the people want and to smooth some of these barriers to accessing services. But, like you have mentioned and based on other testimony that we have heard today, we know that scammers and identity thieves are constantly trying to find new ways to evade ID verification, and that means that *Login.gov* has to remain alert and prepared to fight new forms of fraud. We have to keep innovating.

Ms. Cruz Cain, in GAO's assessment, will there ever be a day when *Login.gov* will be finished and no longer need to adapt to face new fraud tactics?

Ms. CRUZ CAIN. I do not think so. I think criminals are working every day, 24 hours a day, to get better at what they do, and largely in the Federal Government, we are reactive. So, *Login.gov* procured the tools because they are being reactive to what has been

happening within their tools. So, I think largely Federal systems are reactive to what is going on and rather than being proactive.

Ms. RANDALL. Yes. So, would it be safe to say that competent and technically capable leadership of the *Login.gov* program is critical to effectively sustain fraud prevention?

Ms. CRUZ CAIN. Yes.

Ms. RANDALL. And is it critical that leadership has experience in effectively managing and protecting sensitive data programs?

Ms. CRUZ CAIN. Yes.

Ms. RANDALL. Would it be very concerning to you, Ms. Cruz Cain, if leadership at *Login.gov* came from an organization that had, say, an extensive history of mismanaging private data and endangering the privacy and financial security of the American people?

Ms. CRUZ CAIN. Without, I mean, knowing a little bit more about the situation, it would be hard to opine, but we like to look at facts and situations. But, I mean, just like I told you, we would really need to have experience with technology, leadership with good technology, and knowledge of how to implement technology.

Ms. RANDALL. Absolutely. But if someone who had previously been proven to mismanage private data and endanger privacy and financial security was moved into leadership, that would be concerning?

Ms. CRUZ CAIN. Yes, if it was proven.

Ms. RANDALL. Yes. Mr. Chairman, I would like to ask unanimous consent to submit these following articles to the record. "DOGE Put Critical Social Security Data at Risk" from *The New York Times*. From *NPR*, "The Trump Administration Admits Even More Ways DOGE Accessed Sensitive Personal Data." *Washington Post* and *Wired*, similar subject matter.

Mr. SESSIONS. Without objection.

Ms. RANDALL. And just in my remaining time, I would like to say what these articles say, that President Trump took one of the DOGE bros who oversaw the looting of the Federal Government's data and endangered the privacy of every American and put him in charge of identity verification and login systems for every American. And based on our previous line of questioning, that does not sound like a way to safeguard the American people's information.

And I yield back.

Mr. SESSIONS. The gentlewoman yields back her time.

We would now like to move to the second round. With your understanding, we are doing that, sir.

Dr. Maimon, you and I spent some time yesterday. Maybe it was today. Days run together. But you most expressly indicated that you have not only great knowledge, but work on a day-to-day basis with many people who are criminals and who are attempting to be fraudsters at our systems. And I did not have a chance—you did not really delve into this area very much, but I think Mr. Mfume and I need to hear this about not only that it exists, that they are very active, that they are on the dark web or open web, that they target certain people and that they learn areas that are vulnerable, and that they openly talk about it. It is no longer behind anybody's back anymore. Do you mind taking the time that you need to ex-

press the things that we need to understand about the attack that is against us and our agencies?

Mr. MAIMON. With pleasure, Mr. Chairman. As you mentioned, Mr. Chairman, I spent my time, my days infiltrating darknet platforms, Telegram groups, trying to understand what fraudsters put out there and how they bypass a lot of the security solutions that we deploy on financial institutions as well as on the government side. Oftentimes, what we find in those platforms are tutorials, which will walk you through how to bypass many of the security solutions that we have out there. The tutorials sometimes will be offered for free, other times you will pay for them, amounts ranging from $150 to $250, specific guidelines with respect to how to bypass and obtain SBA loans, FAFSA aid. We are seeing, as of earlier this morning, people talking about how to get targets' 401(k) accounts, which I think is a major issue to our country, and we simply see that on scale. We see that, as I mentioned earlier, on darknet and Telegram, but also more and more on Facebook, on Twitter, on Instagram.

A lot of what we see also on—is available on the internet, on the clearnet, websites that the criminal put together and simply offer fake driver licenses for sale. This is the reality that we are dealing with, organized crime groups with very detailed supply chains, which will have our identities offered for sale. They will have services which will allow the fraudsters to build histories around their identities. They will walk you through how to create deepfakes, high-quality deepfakes, both images as well as videos. They will teach you how to take those videos and images and inject them in the cameras of the computers or the smartphone that folks are using in order to apply for benefits or apply for SBA loans and then secure all those resources that they get from the government.

So, this is what we are up against. We are seeing that happen domestically with a lot of organized crime groups operating within the United States, but a lot is happening from abroad as well. We are infiltrating Russian crime groups. We were able to infiltrate some Chinese crime groups who operate the scam compounds in South Asia and are explicit about the type of operations and our identity and how, you know, how they essentially offer those identities for sale and essentially walk you through the list of steps you need to engage in in order to target our benefit program. This is what we are up against, unfortunately, at this point.

Mr. SESSIONS. So, furthering this development that you are talking about, I spoke with you about how we had looked at, during 2021, 2022, 2023, 2024, numbers of agencies that did not have their workers at work. They were not engaging the people who were seeking services. They were not able to, even when working from home necessarily, did not have a full array of opportunities to vet who people were, know your customer, to look at things. And so, this huge amount of money that we were talking about today in testimony before this Subcommittee, that is very consistent with what we have heard GAO say in the past.

It has found a real home to where this is more than a cottage industry. It is people who literally are figuring out how to do this. And you said to me, whenever we last spoke this morning, you do believe human interaction—and I brought up my circumstance of

talking to Social Security, how they vetted me, how they talked to me about things that I would know about myself that probably not a lot of people would understand. Is this the kind of fair game that would be used to vet people on a regular basis? And how can we cross-get this type of information to where if you are at SBA, you may or may not have that available to you? If you are at Social Security, you probably could ask some detailed questions about working history, about doing other things.

Do we need to expand or develop some way for agencies that take a new, perhaps a new, request from a person? It could be about—not VA because you could ask about those questions, but about someone who is recently unemployed and asking about depth of knowledge. How do we really help those agencies make the determination even when speaking to a person?

Mr. MAIMON. This is a great question, Mr. Chairman, and I agree with your statement. I think, and maybe you can go back to my career as sociology in the Ohio State University, first class in the degree, we were taught about the difference between Gemeinschaft and Gesellschaft, community and society. The reason why I am bringing this important distinction is that in the past, here in the United States or any other place, when you went into the bank or to the IRS and asked for opening a new bank account or a loan or getting some governmental benefits, the guy sitting across from you knew who you were. He knew your family. He knew where you worked. He knew your history, so to speak. And so, they were able to assess the risk you posed to the organization more effectively.

Now, you know, we are at this point in a point of a society. We have a lot of people living in this great country, very difficult to assess, in the same way we assessed in the past, folks' history. But fortunately, we do have solutions out there which will allow you to taggle the signals, create and look at some historical signals around identities.

So, if the government is willing to sort of use some of those solutions to try and assess the historical evidence around those individuals who need to be verified, then I think we will be in a better place to sort of determine whether individuals are who they say they are, or they are completely different individuals stealing identities or using synthetic identities.

And in that sense, I just want to refer to the conversation we had earlier about the driver's licenses and MDL. One of the things that we proved already, you know, during the last ten years or so is that pretty much everything could be faked. That, I think, will go also to the MDL. I mean, criminals will be able to find ways to use this technology to their benefit. What they will not be able to fake is the historical evidence.

And that goes as well to the AI solutions out there, right? I mean, AI will be able to give you an amazing picture of a person who does not exist, or AI will be able to take my face and bring it to life when I am abroad, so to speak, and try and authenticate me when I am trying to get unemployment benefits. But one thing that AI tools will not be able to do at this point is to create the historical signals around me or around anyone who is trying to identify themselves.

And I think that is where the solution lies, being able to find solutions which will allow us to look at historical evidence around individuals, around their name, date of birth, addresses, telephone numbers, and make assessments with respect to whether they are who they say they are.

Mr. SESSIONS. Ms. Cain, furthering this discussion, I had a chance to engage you also yesterday, and part of this was about the viewpoint that when there was a failure, meaning a person came through *Login.gov*, provided information, but it was not what I would call successful, so there would be a failure, then, evidently, it is not unusual for someone, not as a challenge, but to ask for authentication of who they are, to go to a post office. You had indicated that one of the things which you have engaged government agencies on, and perhaps GSA, is data and information back about what caused that failure. Was it a question we asked? Was it a picture, any number of facts and factors?

Following up on Dr. Maimon, you are the cybersecurity person also at GSA, and you are aware of the power of technology, the power of these things that could be used to fool people, to give false positives, to do things. Do you see that in this process that we need to go with new areas that would add some more depth to where you did not fail off one or two or three, you failed off five different questions because you were looking for them? How do we go and ascertain when someone falls out, whether that was fraud, whether that was someone you were openly challenging, and they see you later, and so they never went to the post office, and to where we then learn what they did, how they did it, where they asked the question, who they were? We could move them to the organization we talked about this morning, to Pandemic Response Accountability Committee (PRAC).

Ms. CRUZ CAIN. I think it is an important question because the people who are failing and are legitimately the person that they say they are, are going to keep trying because they want that government benefit that they are entitled to.

Mr. SESSIONS. And they could go to a post office.

Ms. CRUZ CAIN. Right, they could go to the post office and go take their documents and verify who they are that way, but there are also barriers to that. So, if you are in a rural area, your post office may be far, you may not have reliable transportation there, there may be lots of barriers for you to do that, so it might not be that easy. So, a lot of the agencies reported to us that they would like to have visibility into that authentication and why it failed, so they might be able to help that person on the end and say, well, yes, it was because the name that you put in was not the name that HUD had on, or there was a letter transposed, or your new address was never updated in HUD's database.

And there was a privacy principle called redress. You know, you are supposed to be able to get the most updated, or whatever information an agency has on you, so you are able to correct it if it is wrong. That process can be easy, or GAO has reported that process can take very long for you to be able to update your information. So, if that takes me months to years to get my address updated in a government database, I am going to fail for that whole year on every government agency that I use *Login.gov* to try to access,

which is going to be a very big barrier for me to get any government benefits that I am eligible for.

So, that was something that many agencies brought up for us. And giving those agencies that ability to—insight into that and to be able to say, hey, this is why you failed, you know, here are your options, and again, some of them may not even be able to go to a post office and have that secondary option available to them, but, you know, you are going to have to do that if you want your benefits. That was one thing that was really helpful to them because some people would—fraudsters would probably legitimately stop. If they were not able to go somewhere and prove who they said they were, nine times out of ten, they are stopped. They will take their other synthetic identities and keep trying to get through, but they would stop probably with that fraud name and say, okay, look, I have got 300 others that I just paid $3 for. I am going to keep pushing those.

So, I think the difference is you really need to think about the people who are really who they say they are, who are having that false positive, that they are going to keep trying, and they need that reason why so that they can go remedy that so they can continue to be—not be found ineligible for the benefits that they are legally entitled to.

Mr. SESSIONS. Okay. Interesting. Thank you.

Mr. Mfume?

Mr. MFUME. Thank you, Mr. Chairman. It has been an interesting hearing, to say the very least.

One of the things that I hope comes out of these sort of interactions are ideas that would affect and change existing law and policy. And I know all of you in your work have come across items, matters, and issues that you said, if this were only changed or if this could be in place. So, I want to come back to that in just a minute, and it will be a quick minute too, but I want you give some thought to that because, as legislators, that is very important to all of us, no matter what side of the aisle we serve on, if we are in fact trying to deal with an issue and a problem, and certainly, this is one of them.

I want to, if I might, Dr. Maimon, go back to something you said earlier, and then I will come back and we will try to wrap this up on this side anyway. I am interested in your work that you have been doing tracking Russian and Chinese cyber networks and their ability to infiltrate this country, but more importantly, their ability to take advantage of the citizens of the United States. It sounds like fascinating work, but I am sure it is also leading you to some ideas about how we can do things better.

What I really want to know, though, on this matter, the evidence that you are coming up with as you track these crime syndicates and cyber networks, whether they are Russian or Chinese, are you or your organization sharing that information with the Director of National Intelligence or sharing it with the FBI, or are they about doing what they do in their own silo, developing their own intelligence and not doing a comparative analysis of both? Could you speak about that for a minute?

Mr. MAIMON. Of course. Thank you so much for this question. I do what I do in order to make sure that the American public is

aware of what is going on there, and when I investigate, my investigations usually result in publications. I put together white papers; I put together news articles and let the public know about what I find.

Oftentimes, we will reach out to law enforcement, and then we will simply give it to them, and then they need to make a decision with respect to whether they want to pursue an investigation or not. I can tell you that in the past, we had a very strong relationship, as a professor in Georgia State University, with the Department of Homeland Security. What we have done back then, that was during the pandemic time, we essentially had a monthly meeting with local folks in DHS, and we simply talked about what is it that we find out there. What is it that the Department of Homeland Security (DHS) did with that information? Obviously, I have no idea because, oftentimes, what happens is that law enforcement takes this information and do their own thing, sort of speaking.

And so, I can tell you that I am doing my best to make sure that everybody is aware of what I find out there, but I have limited visibility with respect to the actions folks take once I put information out there.

Mr. MFUME. Well, if I could be the devil's advocate, if I am the Director of National Intelligence or the head of the FBI, I might say, well, he has never given that information to us. So, do you forward that to them? Are you in contact? Is there a liaison that shares the information so they can match it up with their own intelligence?

Mr. MAIMON. So, in the past, what I was doing is essentially having a monthly meeting with the Department of Homeland Security. That was during COVID time. We had a very strong relationship at the time, where we essentially provided——

Mr. MFUME. Right, but I am specifically speaking about the Director of National Intelligence and the Federal Bureau of Investigation.

Mr. MAIMON. Yes, I do not have a relationship with the FBI. I do not stay in touch with the FBI. I am more than happy to be in touch with them and let them know about what I know.

Mr. MFUME. Yes, because it seems like you have done an extensive amount of work, and I can appreciate white papers and editorials and that sort of thing, but everybody does not read, and if it is something so pertinent or hot or game-changing, those two agencies, more than anyone else, I think, needs to know. So, let us pray that they are listening. They obviously are. I hope that they would take advantage of the work that you have already done just to match it up against their own intelligence. This is a very serious issue, as we all agree, and the more we can do to be effective, the better.

And now, I just want to come back to all of you, just very briefly, with respect to this notion about policy changes or about proposed legislative avenues to address some of the more glaring aspects of this, or maybe just to address things that right now are not getting any attention. I am going to start with you, Mr. Burris, and I will end up with you, Mr. Stanley.

Mr. BURRIS. Thank you, Ranking Member, for the opportunity to address this item. You know, there were a number of recommenda-

tions that I provided as part of my testimony as far as where we could be pursuing policy levers. I actually will lead with one that was not in there, and it is really around mindset shift and culture. And if you indulge me for just a moment, it shows you the depth of my nerd.

It goes into—I was thinking actually back to the *Avengers* movie, the last one with Captain America, and how there was like the darkest moment where they were basically up against an insurmountable threat, basically took all the Avengers coming together at the same time out of nowhere in order to try to combat what they were seeing or what was about to happen. I think that generally, culturally, has to change within the Federal Government in the sense that right now, when you are talking about who is fighting fraud within an agency, an organization, they are doing it siloed. They are doing it without sharing intelligence. They are doing it without having the types of conversations that need to happen, so much so that Federal Emergency Management Agency (FEMA) could be having an existential fraud threat, and they are not talking to the SBA. They are not talking to Treasury. They are not talking to GSA even. And so, there is an opportunity to basically culturally shift to say that we all have to get on the same page about what we are fighting against and then change that dynamic so that way we can actually can take some of these more proactive measures that I have outlined in my testimony.

Mr. MFUME. Thank you very much. I appreciate that. I did not see the movie, but I appreciate your context. But I am talking now about policy more so than mindset. Mindset is going to take a while, but if we can implement minor or major policy changes, that will make a difference right now.

Ms. Cruz Cain?

Ms. CRUZ CAIN. I will go for a big one, but I think we do need to revamp the Federal Privacy Act. So, the Privacy Act goes back to 1974. GAO has plugged many times in its reports that that was created way before policy and technology has updated, and we need to revisit that. But I also think that there is a great need for a consumer privacy law as well that starts at the Federal level but also allows states to have some input into it because of, right now, there is no Federal consumer privacy law, and it is a sort of framework of mismatched state laws, local laws, and, you know, there is nothing really governing at a higher level of what needs to be done.

Mr. MFUME. Thank you.

And Dr. Maimon, I appreciate the extensive nature of your written remarks. I tried to get through all 20 pages. I do not know if I did or not, but thank you very much for that.

Mr. MAIMON. Thank you so much. I think in terms of policy—and I really appreciate this question because I sit at Georgia State University in the School of Policy. One of the things that I would strongly recommend is an evidence-based approach. I think, you know, we are in a point in time where science has advanced dramatically. We have evidence-based medicine, evidence-based policing, all essentially suggest that in order to make decisions with respect to policy or the implementation and tools, what we need to do is essentially test what works and what does not.

Unfortunately, we do not have that in the context of fraud. So, I think if we are thinking about policies and policy changes, the first thing we need to sort of have in mind is a different state of mind, and that is of evidence-based, what works and what does not in the context of fraud prevention.

In the context of the government operation, we are in a very difficult position, I would say, because, to be honest, we do not really know how much fraud we have. We have reports on improper payments, but we do not know how much fraud we have on the government side. We hear numbers and very large numbers, so it is definitely an issue, but we need to be able to quantify how much fraud we have. And then after we quantify that number, we need to try and assess how to reduce that number to the minimum possible in order to make sure the taxpayers get their money's worth in terms of benefits, in terms of programs that they should have access to.

So, I think if we need to sort of have something in mind when we think about a policy change, then it is definitely an evidence-based approach to fighting fraud.

Mr. STANLEY. [Off mic.]

Mr. MFUME. Mr. Stanley, could you turn your mic on, please?

Mr. STANLEY. I am so sorry about that. I would agree with Ms. Cruz Cain that strengthening the Privacy Act of 1974 is sorely needed, as well as overarching consumer privacy legislation. I believe that the United States is the only advanced industrial Organization for Economic Co-operation and Development (OECD) nation that does not have an overarching privacy law that sets baseline expectations for both individuals and businesses about what is fair and what is not in terms of how people's information is treated.

And then, as I have been arguing, I think that we need to set standards for digital driver's licenses in the states and other digital IDs that put in place both requirements for how they are built technically. They should have certain encryption capabilities that protect privacy while still allowing for people to authenticate themselves. And there should be an envelope of legal protections around them to make sure that they remain optional and not mandatory, for example, and to limit overuse. And so those would be the top things that I think the Congress should consider.

Mr. MFUME. Thank you very much. I want to thank all of you.

Mr. Chairman, you may recall this idea of revamping the Federal Privacy Act continues to come up. The last hearing we did like this, that same thing came up. So, I want to commit myself, and I am sure, you know, you and I will get together on this and figure out how, in fact, we might be able to move forward with some joint legislation that at least starts to move the ball regarding the Federal Privacy Act. It has been a long time since 1972. The world has changed, and the least we can do, I think, is to try to find a way to protect the privacy of Americans by updating the Federal policy that we have. And I want to commit myself to working with you in that regard. I yield back.

Mr. SESSIONS. The gentleman yields back his time. Was that your closing statement also?

Mr. MFUME. Yes.

Mr. SESSIONS. The gentleman did make a closing statement.

I, too, want to join in with my dear friend, Mr. Mfume, and thank each of you for being here. This issue is not going to go away. The question is, are we serious enough to continue the search to look for these things? And I think all four of you have proven to us today that there is not just much ground to go, but there is much to learn.

And I think both Mr. Mfume and I need to provide some, perhaps, guidance back to inspectors general, their attention to this, to help GAO to reinforce the things that they are after, to have the GSA follow-up. I find myself in a position where I do not want to say that they are not paying attention. I think they are trying to do a number of things that are important. But Mr. Mfume and I find ourselves on this end of the trying to save the taxpayer, trying to understand that the people, whether it is one of my sons or it is one of his constituents, that need government benefits and government services to work properly, to be legally bound to recognize these things, but that we will bleed ourselves out. We can bleed ourselves out by people who are outside the system, causing us to completely miss the mark.

So, we are going to stay after this. We are going to make sure that we approach every single angle and challenge government to do that. We have, by and large, decided we do understand the PRAC. We do understand the importance of data. We do understand the need to make sure that it survives in perpetuity, yes, probably for a lot longer, that we give it the authority and the responsibility to evolve itself, to meet the emerging and new threats, and to provide information back.

But, I want to thank you for your insistence that we will continue to work together, and I want to thank each of you.

So, with that said, without objection, all Members have five legislative days within which to submit materials and additional written questions for the witnesses, which would be forwarded to the witnesses.

If there is no such further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:58 p.m., the Subcommittee was adjourned.]