AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 117–586

PROTECTING CONSUMERS FROM FINANCIAL FRAUD AND SCAMS IN THE PANDEMIC RECOVERY ECONOMY

HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER PROTECTION

OF THE

COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE FINANCIAL SCAMS FOLLOWING THE COVID–19 PANDEMIC AND THEIR IMPACT ON FAMILIES AND CONSUMERS IN THE RECOVERING ECONOMY

AUGUST 3, 2021

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: https://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
51–115 PDF WASHINGTON : 2023

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chairman*

JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
TINA SMITH, Minnesota
KYRSTEN SINEMA, Arizona
JON OSSOFF, Georgia
RAPHAEL WARNOCK, Georgia

PATRICK J. TOOMEY, Pennsylvania
RICHARD C. SHELBY, Alabama
MIKE CRAPO, Idaho
TIM SCOTT, South Carolina
MIKE ROUNDS, South Dakota
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
BILL HAGERTY, Tennessee
CYNTHIA LUMMIS, Wyoming
JERRY MORAN, Kansas
KEVIN CRAMER, North Dakota
STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*
BRAD GRANTZ, *Republican Staff Director*

CAMERON RICKER, *Chief Clerk*
SHELVIN SIMMONS, *IT Director*
CHARLES J. MOFFAT, *Hearing Clerk*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER PROTECTION

RAPHAEL WARNOCK, Georgia, *Chair*
THOM TILLIS, North Carolina, *Ranking Republican Member*

ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
CATHERINE CORTEZ MASTO, Nevada
CHRIS VAN HOLLEN, Maryland
KYRSTEN SINEMA, Arizona

RICHARD C. SHELBY, Alabama
TIM SCOTT, South Carolina
MIKE ROUNDS, South Dakota
BILL HAGERTY, Tennessee
CYNTHIA LUMMIS, Wyoming
JERRY MORAN, Kansas
KEVIN CRAMER, North Dakota

ANNIE WANG, *Subcommittee Staff Director*
RYAN ADAMS, *Republican Subcommittee Staff Director*

C O N T E N T S

TUESDAY, AUGUST 3, 2021

	Page
Opening statement of Chairman Warnock	1
Opening statements, comments, or prepared statements of:	
Senator Tillis	3
Chairman Brown	5

WITNESSES

Liz Coyle, Executive Director, Georgia Watch	6
Prepared statement	21
Responses to written questions of:	
Senator Cortez Masto	42
John Breyault, Vice President of Public Policy, Telecommunications, and Fraud, National Consumers League	7
Prepared statement	21
Responses to written questions of:	
Senator Cortez Masto	42
Rachel Greszler, Research Fellow, The Heritage Foundation	9
Prepared statement	29

PROTECTING CONSUMERS FROM FINANCIAL FRAUD AND SCAMS IN THE PANDEMIC RECOVERY ECONOMY

TUESDAY, AUGUST 3, 2021

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER PROTECTION,
Washington, DC.

The Subcommittee met at 2:34 p.m., via Webex and in room 538, Dirksen Senate Office Building, Hon. Raphael G. Warnock, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF CHAIRMAN RAPHAEL WARNOCK

Chairman WARNOCK. This hearing will now come to order. Welcome to the first hearing of the Subcommittee on Financial Institutions and Consumer Protection in the 117th Congress.

This hearing is in a hybrid format. Our Members are in person, but we will have witnesses testifying both in person and by video. We are grateful for their presence.

For those joining remotely, just a few reminders: Once you start speaking, there will be a slight delay before you are displayed on the screen. To minimize background noise, please click the mute button until it is your turn to speak or ask questions. You should have one box on your screens labeled "clock" that will show how much time is remaining.

As we are all here in person, our speaking order will be as is traditional, that is, by seniority of the Members here when the gavel came down and then by seniority of Members arriving later, alternating between Democrats and Republicans.

I am deeply honored to chair the Subcommittee and to work with Ranking Member Tillis to ensure stability in our banks, credit unions, and other financial institutions that serve families and communities in Georgia and all across our country and to ensure that consumers are protected from unfair, abusive, and deceptive acts and practices in our financial system, including financial scams and fraud.

And this brings me to the topic of our very first hearing today, which will examine financial scams following the COVID–19 pandemic and their impact on families and consumers in the recovering economy. Needless to say, the economic turbulence of the last year has pushed working American families to the brink, forcing them to choose sometimes between their health and their liveli-

hoods. According to the Federal Reserve, one in four Americans reported at the end of last year that they were financially worse off than they were the prior year. This is the highest level since 2014.

Compounding these economic setbacks has been the rise of scammers shamelessly seeking to take advantage of working families trying to navigate the pandemic, including already vulnerable populations like senior citizens, communities of color, our servicemembers, and veterans. For instance, when I held a teletown hall a few weeks ago with AARP, one woman from Georgia told me that she was receiving three to five scam callers per day. Scammers target these populations because they know that families are desperate, clawing their way back from a pandemic.

And despite the help provided by the American Rescue Plan Act, many families still face limited economic opportunities during this recovery as they watch their debt pile up. Naturally, they are looking for help.

And here are just a couple of examples of how scammers are stepping in to take advantage of these vulnerable moments of economic uncertainty: Just a month ago, the CFPB and the Georgia Attorney General's Office took action against the Burlington Financial Group, a company that falsely promised its services would eliminate credit card debt and improve credit scores. The company charged monthly fees that amounted to as much as 40 percent of the debt owed, collecting thousands in fees from desperate Georgians trying to grapple with mounting credit card debt.

And what did consumers get in return for all of those fees? They only got generic form letters to send to their creditors, thousands of dollars in fees for a useless piece of paper. Many customers never got a dollar of their debt reduced, and in some cases they ended up in a worse financial position than before.

In another case from just 2 weeks ago, the CFPB took on a Georgia-based corporation, GreenSky, that took advantage of families trying to make necessary repairs to their homes. This loan app was supposed to help families access loans for home repair services. Instead, it allowed businesses to take out loans on behalf of customers without their permission or knowledge. GreenSky was operating before the pandemic took place, but the group of consumers that they exploited, who lacked access to traditional credit markets and relied on digital tools to conduct financial transactions, was a population that grew dramatically during the pandemic.

Additionally, we know Federal benefits are often prime targets for crooks and scammers have set their sights on struggling families receiving Federal help from the American Rescue Plan. One scam we have seen frequently in the last year occurs when scammers actually impersonate Government officials and claim that consumers need to hand over personal information to access Federal support, like their COVID–19 relief check or child tax credit. These scammers sometimes falsely claim that consumers need to, quote, refund the Government for their benefits.

And coupled with these increased opportunities for scamming are new tools and financial platforms that enable these scams. Due to the pandemic, more and more Americans are engaging in financial transactions on new peer-to-peer, online payment platforms like Cash App, Venmo, whose terms are often unclear and lack critical

protections for consumers. Unlike traditional debit or credit cards, many of these platforms offer only limited protections against scams, leaving many users caught unaware that they have been defrauded. These platforms make it easier for scammers to swindle consumers out of thousands of dollars, with little to no mechanism to hold their scammers accountable. In some cases, a consumer could simply put in one wrong number or hit one wrong button and their money is gone forever.

Collectively, these frauds swindle countless dollars from the most vulnerable members of our society: seniors, marginalized communities of color and other communities that are marginalized, our veterans, members of the military. And most heartbreaking of all, many individuals who fall prey to these sophisticated criminals face barriers in reporting these crimes and holding the perpetrators accountable. Not only are consumers often embarrassed to admit that they have been victimized, but they may also not know what resources are available to remedy their losses, and even then, investigations can take years to deliver justice.

Here is what I believe: I believe that Congress, and this Subcommittee in particular, has a role to play in protecting these consumers and preventing scammers from taking advantage of more Americans. And so I am looking forward to hearing from our witnesses today to learn more about today's financial fraud and scams, and how financial institutions, Congress, and Federal regulators, including the Consumer Financial Protection Bureau, can take action to curb financial fraud and scams. That is our work, particularly scams involving companies, payment platforms, and other financial institutions that are under this Subcommittee's jurisdiction. That is what this hearing is about.

This hearing is about helping people. Hardworking American families have already suffered enough from the pandemic, and as their economic situation recovers, we cannot allow their hard-earned dollars to be siphoned off by scams and cons. Thank you.

And I will now turn to Ranking Member Tillis for his opening statement.

OPENING STATEMENT OF SENATOR THOM TILLIS

Senator TILLIS. Thank you, Chairman Warnock, and for holding this hearing, and thanks to the witnesses present in the chamber and connecting remotely.

I absolutely believe that fraud is despicable and illegal and should be pursued vigorously and relentlessly. I have seen countless hearings when I was on the Aging Committee about how seniors were being exploited. I am sure many other committees will hear the same thing.

But I do want to be clear. Some of what we are going to hear today lies outside of the Committee's jurisdiction and the jurisdiction of financial regulators. The understandable desire to bring bad actors to justice should not be an excuse to further broaden the scope of Federal regulators' purview. Not all fraud is financial services fraud. Given the CFPB's history on overreach, I believe that is worth pointing out.

I also believe that any conversation regarding protecting consumers from fraud and scams must include unemployment insur-

ance fraud, UI fraud. Recent reporting is beginning to shed light on the size, the scope, the implications of this fraud although the full toll is likely not to be known for some time. And, Mr. Chairman, I would like to seek unanimous consent to put forth an article from ProPublica that gives you jaw-dropping numbers on just the extent of the UI fraud.

Chairman WARNOCK. Without objection.

Senator TILLIS. Thank you. The Department of Labor's Office of Inspector General placed the prepandemic and proper payment rate for Federal UI system at 10 percent. It is one of the highest rates in the entire Federal benefits system. Extrapolating this rate out to all Federal dollars spent on UI, which is expected to be about $873 billion by program end, it gives a total of $87.3 billion of improper payments during the COVID era. $87.3 billion is roughly 4 times the annual NASA budget.

If $87.3 billion was the full extent, this would be a problem, a major one, but not necessarily a scandal. But DOL's Inspector General acknowledges the $87.3 billion is likely far too conservative. Analysis of the total number of UI claims compared to the number of unemployed individuals in the U.S. during COVID led researchers to place the amount of UI fraud far higher, at $357 billion or 40 percent of the entire program. Even worse, a unit for research in news corporation Thomson Reuters believes 40 to 50 percent of claims they analyzed are highly suspect for fraud.

And I do want to maybe deviate from my comments for a moment. We are not talking about individuals, fraudulently. We are talking about organized crime and a number of organizations who have bilked the Federal Government and are going to create disastrous consequences for what would ostensibly be the recipients of the UI benefit.

If one adds the $166 billion that States contributed to UI during the pandemic, the estimated total for the entire program surpasses $1 trillion. A fraud rate on this total, similar to the Thomson Reuters projection, would mean somewhere between $400 and $500 billion in fraud or between 50 to 65 percent of the entire annual Defense budget. That is a scandal. It is one of epic proportions.

But aside from the egregious waste of taxpayer dollars, why should the average American be concerned? Because there is a real change their identity was stolen and used to file fraudulent claims. Many experts see online hacking and identity theft as foundational to any conversation of COVID-era UI fraud. Over the past several decades, hackers have systematically stolen personally identifiable information, PII, from the Government and private data bases alike. The Privacy Rights Clearinghouse identified nearly 2,300 verified hacks from 2010 to 2019, which disclosed almost 6.9 billion personal records.

And while the availability and the ease or procurement of stolen PII has accelerated over the past several years, it increased exponentially during the pandemic. During 2020, the Federal Government saw a 2,900 percent increase in consumer complaints filed that someone's identity had been stolen and used to file fraudulent Federal benefits.

This rise in fraud is driven by bad actors and, as I said earlier, criminal organizations and individual actors. Research into dark

web forums found at least 25 different platforms with users compiling and/or selling private information. Several have thousands of participants, and they offer stolen identities for sale, tips for bypassing the antifraud protections of State UI system and how to do it, and often including feedback on which States are easiest to scam.

In 1 month in Vermont, they determined—the State of Vermont determined 90 percent of UI claims—I am sorry, these were independent investigators—were likely fraudulent, 90 percent, likely the result of identifying the States that are the easiest targets. Likewise, a single State working with Thomson Reuters' fraud detection group received fraudulent claims from IP addresses that were traced back to nearly 170 countries around the world.

Analysis reveals digital footprints that indicate foreign workers, mostly commonly in China, Brazil, Mexico, and West Africa, have been hired by sprawling and often highly organized criminal enterprises to systematically and repeatedly and effectively use stolen American identities to claim UI benefits.

America needs to be made aware of the fraud—of this fraud, and Congress must work to carefully craft policies in the future that do not jeopardize Americans and their personal information. It is imperative that we examine this fully to ensure that Government programs, without necessary programs, do not become a windfall for scammers and fraudsters alike again.

And when I get in my questions, I want to talk about some of the impacts, Mr. Chairman, I think many Americans are going to have next year when they are filing taxes or they get audited a year or two from now for having not claimed income that they had no earthly idea was claimed in their name. Thank you.

Chairman WARNOCK. Thank you very much, Ranking Member Tillis.

The Chairman of our Committee is here. Chairman Brown will offer remarks.

OPENING STATEMENT OF CHAIRMAN SHERROD BROWN

Chairman BROWN. Thanks and I will be brief. And thank you, Mr. Chairman, Senator Tillis. Thanks for doing this hearing. You said the first hearing of your Subcommittee, so congratulations.

The COVID–19 pandemic has claimed the lives of more than 600,000 Americans. We have made great progress getting shots in arms, but we are experiencing surges in areas across the Nation we know that have low vaccination rates. It is important we continue to provide families with the resources they need to protect themselves and their loved ones, both medical resources, like vaccines that will save their lives, and also economic resources as the economy continues to fully recover.

While we all hope to avoid, and must work to prevent, a future pandemic, we also need to protect American families from those who would use a public health emergency and use an economic crisis as an opportunity to defraud and exploit them. We have seen Americans reach out to the Consumer Financial Protection Bureau in record numbers with complaints about credit reporting companies and banks and debt collectors. We have also heard from CFPB and other Federal agencies that scammers are targeting student

loan borrowers and homeowners and working families who are receiving advanced payments of the child tax credit.

I look forward to working with my colleagues from both parties to highlight what we can do to protect workers and their families. No one should have their financial future ruined because of a global pandemic. Thank you, Mr. Chairman.

Chairman WARNOCK. Thank you very much, Chairman Brown. Let us now turn to our witnesses. Testifying today will be:

Ms. Liz Coyle, the Executive Director of Georgia Watch. Founded in 2002, Georgia Watch is the State's leading nonprofit, consumer advocacy organization. Georgia Watch advocates for policies that open doors to the financial mainstream, increase individual and family economic security, improve access to affordable health care, and lower the energy burden on struggling families.

Also testifying is Mr. John Breyault. Is that correct?

Mr. BREYAULT. Yes, sir.

Chairman WARNOCK. I want to pronounce your name correctly. A nationally recognized consumer advocate with more than 18 years of experience championing the rights of consumers and the underserved.

Finally, our last witness is Ms. Rachel Greszler, a research fellow at the Heritage Foundation, and she focuses on retirement and labor policies.

We appreciate your testimony, and we look forward to our discussion. Ms. Coyle, who is testifying virtually, I will now turn things over to you.

STATEMENT OF LIZ COYLE, EXECUTIVE DIRECTOR, GEORGIA WATCH

Ms. COYLE. Good afternoon. Thank you, Chairman Warnock, Ranking Member Tillis, for inviting me to speak before this Subcommittee today. I am truly honored to have this opportunity.

As Members of this Subcommittee know, our country still is facing significant health risks tied to COVID–19 and recovery from the pandemic economy remains challenging for many and fraught with obstacles and dangers for the most vulnerable among us. Today, we are here to talk about protecting consumers from scams and fraud in the pandemic recovery economy. I am grateful to the Committee for shining a light on this issue.

I would like to share with you today some of my concerns as a consumer advocate from Georgia. Every day, we work to help Georgians with the issues that impact their lives and livelihoods. The pandemic public health and economic crises further heightened what we already knew. Those already struggling to access needed health care, keep the lights on, pay off debts, and live in stable housing would be much more significantly impact by the challenges suddenly confronting all of us. Our toll-free consumer hotline started ringing on day one of this crisis, and we continue to hear regularly from people needing assistance. This especially is the case among our seniors on fixed incomes, veterans, lower-income households, and communities of color, who have long been disparately impacted in times of crisis.

We knew many consumers in Georgia were facing—were feeling desperate and vulnerable. Bad actors definitely knew that, too.

From the early days, scammers and fraudsters plotted to benefit substantially from these conditions, and as we have learned from Federal and State regulators, they did.

While many of today's scams look a lot like yesterday's, a new kid on the economic block may be having an outsized influence on the current shape of fraud. Emerging financial technology tools certainly offer convenience and, for some under- and unbanked Americans, access to the mainstream economy, which is good. However, these fintech offerings may also be used by bad actors to facilitate scam-based theft. For example, a mobile lending technology developed by a company from Georgia has been used by home repair scammers as the perfect vehicle to steal from unsuspecting, vulnerable homeowners. And Chairman Warnock touched on this in his opening remarks.

We also have heard from consumers who have been scammed when using a common social media platform, Facebook, that has been around for a very long time. We know that scammers use Facebook to steal money from unsuspecting consumers. Someone might see an ad while using this platform and be tricked into purchasing a product from a fake company. When the merchandise does not come, they are left with nothing more than a web address and maybe an email address to a fraudulent, nonexistent company.

In closing these remarks, I want to acknowledge the vitally important role played by the Georgia Attorney General and Department of Law and the Consumer Financial Protection Bureau in alerting us to emerging scams, and there are new ones that we are alerted to practically every day. Notably, these regulators both launched investigations and initiated enforcement actions related to those home improvement scams you have already heard about today.

I recommend that policymakers ensure our State and Federal regulators have the authority and the tools they need to regulate effectively and enforce rules as necessary to protect consumers and keep the emerging fintech marketplace safe for all. And I want to thank you again, Chairman Warnock and Ranking Member Tillis, for inviting me to speak before this Committee today.

Chairman WARNOCK. Thank you so very much, Ms. Coyle.

Next, we will hear from Mr. Breyault.

STATEMENT OF JOHN BREYAULT, VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS, AND FRAUD, NATIONAL CONSUMERS LEAGUE

Mr. BREYAULT. Good afternoon, Chairman Warnock, Ranking Member Tillis, and Members of the Subcommittee. My name is John Breyault, and I am the Vice President of Public Policy, Telecommunications, and Fraud for the National Consumers League. Founded in 1899, NCL's nonprofit mission is to advocate for social and economic justice for consumers and workers in the United States and abroad. I appreciate the opportunity to speak to you today about how fraud linked to the COVID–19 pandemic and recession has affected vulnerable consumers and the role that peer-to-peer, or P2P, payment technologies have played in exacerbating that harm.

To put it bluntly, the COVID–19 pandemic has been a perfect storm for scams. By almost any measure, rates of fraud related to the pandemic have mushroomed. In 2020, the Federal Trade Commission received 4.8 million fraud complaints, more than at any time in its 106-year history. Consumers reported $3.4 billion in fraud losses to the FTC, with a median loss of $306. These numbers are widely acknowledged to be only the tip of a massive iceberg when it comes to fraud perpetrated during the pandemic. And just as deaths, illnesses, and job losses related to COVID–19 have fallen hardest on historically marginalized communities, so too has the impact of fraud linked to the pandemic fallen disproportionately on consumers of color.

The ultimate goal for fraudsters is stealing money. Scammers routinely take advantage of new financial technologies to facilitate the transfer of funds. While no financial institution wants to be used as a vehicle for crime, there is often tension between businesses' desire to secure a particular payment vector from fraud while still allowing for legitimate transactions to be processed quickly. This tension is clear when it comes to the rapid growth of P2P payment platforms such as PayPal's Friends and Family and Venmo services, Square's Cash App, and Zelle, which is owned by a consortium of major banks.

These services have attracted tens of millions of users by allowing for free or very low-cost payments to be sent between consumers or from consumers to businesses. Even before the pandemic, roughly four in five Americans had used mobile payment apps by one estimate. By 2023, it is estimated that more than $1 trillion will be transacted by P2P apps annually.

Unfortunately, the same features that are fueling the rapid growth of P2P apps, namely, low-cost, instantaneous payments made via smartphone have made P2P a payment method of choice for scammers. Analysts estimate that fraud rates on these platforms are three to four times higher than for traditional methods such as debit or credit cards.

Despite the platforms' efforts to educate users about the risks of sending money via their platforms, more than half of consumers surveyed by AARP incorrectly assume that their payments would be protected if there is an error or fraud associated with the transaction. While no financial service is immune from fraud, protections for consumers who lose money to scammers on P2P apps are sorely lacking. A big reason for this is the loophole in the Electronic Fund Transfer Act that excludes payments initiated by the consumer from the protection for unauthorized charges. This is also known as "fraud in the inducement" or "victim-assisted fraud." This allows P2P services and banks to avoid liability for payments sent from consumers to scammers even when such payments are induced by fraud.

The end result of this loophole is that the liability risk for fraud is transferred from the platforms and banks to consumers themselves. The only recourse for many victims of fraud committed via these apps is to throw themselves at the mercy of the banks or platforms and beg to be made whole. Unfortunately, thanks to the lack of legal protections, it is far too easy for the banks and P2P apps to simply tell fraud victims that they are out of luck. And,

Senator, we hearing from these consumers with these stories every day at NCL.

To ensure that P2P apps are secure for their users and do not continue to be powerful tools for fraudsters, action by Congress is urgently needed. My written testimony includes a number of legislative actions to strengthen protections for consumers using P2P apps. In particular, I would like to urge the Members of the Subcommittee to work to enact legislation that expands the EFTA's definition of unauthorized electronic fund transfer to cover fraudulently induced payments, with ultimate liability resting with the institution that received the fraudulent payment. Doing so would give consumers the confidence that they would be made whole if they are induced to send money to scammers via P2P services. It would also create a strong incentive for all stakeholders in the P2P payment ecosystem to make security a priority just as it is in the debt and credit card space.

In conclusion, Chairman Warnock, Ranking Member Tillis, on behalf of the National Consumers League, thank you for continuing your work to protect consumers and for holding today's hearing. I look forward to your questions.

Chairman WARNOCK. Well, thank you so very much for your work in this sector and for bringing that experience to your testimony.

Ms. Greszler will testify in person.

RACHEL GRESZLER, RESEARCH FELLOW, THE HERITAGE FOUNDATION

Ms. GRESZLER. Good afternoon and thank you for the opportunity to testify today. Having closely followed the expansion in unemployment insurance benefits since the pandemic, I would like to focus my remarks today on some of the unintended consequences of those expansions, which serve as a caution against future expansions and also a caution against the creation of new Government benefit programs.

It was clear from the outset that certain components of the unemployment expansion were problematic, including the $600 and now $300 weekly bonus payments, that both prolonged unemployment and also contributed to the current labor market shortage by making it advantageous for some people to be unemployed as opposed to employed.

But what was not anticipated was the massive increase in fraud in these UI programs. Unemployment benefits are supposed to be reserved for individuals who lose their job through no fault of their own, and employers are supposed to verify that individuals have lost their jobs. But the expansions effectively required States to base eligibility determinations on self-certification information, which made it relatively easy for criminals to steal information and Government benefits. And it certainly did not help that many Government benefit programs operate on decades-old technology that makes it hard for them to adapt quickly and also to prevent fraud.

In a single year, the number of identity theft reports filed with the FTC by individuals who had their information used to obtain Government benefits or Government documents increased 27-fold. It went from 23,000 identity theft reports the year prior to the pan-

demic to 637,000 the year after the pandemic, and that is only the people who know that their identity was stolen and who actually filed a report because of it.

Instead of just helping individuals who lost their jobs and incomes, much of the UI expansions have instead fueled fraud. My analysis of the Department of Labor's data shows that the total number of UI benefits sent out between April 2020 and May 2021 was 1.36 billion checks. But had the programs simply covered 100 percent of unemployed workers, which was an ambitious goal, 807 million checks would have been needed. That means that 557 million benefit checks, equal to $357 billion worth of taxpayers' money, went to individuals, mostly criminals, who were not actually unemployed.

While States have undertaken efforts to update their technology and to prevent fraud, some States' actions have instead fueled fraud. For example, California's Employment Department sent out 38 million pieces of mail containing individual Social Security numbers since the start of the pandemic, and this was after a 2019 State auditor report advised them to stop that practice.

And unfortunately, Government programs themselves are not immune to compromise. Massive data breaches across State revenue departments, within military medical systems, and at the Office of Personnel Management have resulted in tens of millions of Americans having their personal information compromised.

UI expansions were supposed to last for about 5 months, but instead they are track to last for about 18 months. And despite these unintended consequences and the surge in fraud, many policymakers want to make parts of these UI expansions permanent and also to add new Government programs, but these things would simultaneously up the ante for criminals and also create new avenues for individuals' and children's personal information to be exploited.

Even prior to the pandemic, Government benefit programs had incredibly high rates of fraud and improper payments, including 12 percent in the child tax credit and 24 percent in the earned income tax credit. Creating child payments that are worth up to $3,600 per year, while eliminating the income requirements and converting them into monthly benefits, will almost certainly increase errors and fraud. And other benefit programs, like a Federal paid family leave program, childcare subsidies, would add new privacy concerns. Along with the creation of these programs would be new data bases, and there would be requirements for employers, and for private childcare and medical providers, to collect and to transmit personal information such as health records, children's Social Security numbers.

So rather than requiring individuals to pay higher taxes and disclose their personal information to multiple Government agencies, in order to receive what politicians think they need to provide for their families, instead, lawmakers should let Americans keep and freely save more of their own money so that they can use it on the things that they want and need without the restrictions of Government programs and without putting their personal information at risk. Allowing individuals to save in universal savings accounts is just one measure that would help this goal. Thank you.

Chairman WARNOCK. Thank you very much. We will turn now to questions. We are grateful to all of the witnesses for their testimony.

Last month, thanks to the American Rescue Plan, over 2 million Georgia children began receiving the $300 per month child tax credit. Experts tell us that this will cut child poverty up to 50 percent in our country. Eradicating childhood poverty is an issue that touches me deeply. It emerges from my own experience and my own faith. And championing this tax cut has been one of my proudest moments in the Senate. I think ordinary folks, working class people, poor people deserve a tax cut.

The child tax credit not only helps give working families financial stability and peace of mind; it boosts the economy for all of us. But unfortunately, cybercriminals have been targeting this benefit as they target all benefits. The IRS recently warned parents of fraudulent phone calls, emails, and text messages asking for their personal information. Other scammers have pretended to be the IRS, and even parents, for payment via gift cards, wire transfer, or cryptocurrency to receive the benefit.

Mr. Breyault, what can lawmakers do to protect families from these types of phishing scams?

Mr. BREYAULT. Senator, thank you for the question. What can happen is that the Senate could consider legislation and other protections that would better secure the payment technologies that scammers are relying on to—when money is sent from them—from consumers to the scammers. So for example, I mentioned changes that could be made to better secure P2P payment apps. I will tell you that, for example, Cash App, which is one that I mentioned and I believe you mentioned in your opening remarks, is now being used to buy cryptocurrency. From a scammer's point of view, this is almost the perfect tool for them to use. So considering legislation that would better protect those vulnerable payment vectors is one way to go about better protecting consumers when they are eligible for these types of benefits that you described.

Chairman WARNOCK. Thank you so much. As families continue to receive the child tax credit, I think it is important for us to monitor these types of fraud reports and to work to ensure that families who deserve the tax cut, for whom it was determined, are actually receiving the tax cut.

I have got a couple more minutes. I am proud to say that Georgia has long been a national leader in the fight against predatory lending. Georgia imposes a strict 10 percent usury limit on small-dollar loans. Almost 1 in 10 Georgians is a veteran. Every one of them deserves protection against predatory mortgage lending markets.

Last year, the CFPB issued a civil penalty against a company that was found to have consumers' mailers for mortgage lenders guaranteed by the Department of Veterans Affairs that contained false, misleading, and inaccurate information. This is not the first company doing things like this, and sadly, it probably will not be the last.

Ms. Coyle, what can be done to ensure that Georgia's veterans and veterans all across our country, servicemembers, military families do not fall victim to scams like this one, who prey on those in uniform?

Ms. COYLE. To——

Chairman WARNOCK. Ms. Coyle, you are on mute. If you could start again.

Ms. COYLE. Our nice technical helper, Mr. Moffat, has gotten me out of trouble once again.

Thank you, Chairman Warnock, and I only—I have a minute to say that, yes, we are the proud home to many veterans, servicemembers, and their families. And we know, tragically, that some of these predatory, bad actors prey on them. We know that car title lenders, for example, cluster around military bases. And we are very pleased that the Department of Defense a couple of years ago updated the Military Lending Act. The Consumer Financial Protection Bureau is a great resource for our servicemembers.

Right now, we are concerned about scammers who are going after veterans and their surviving spouses, trying to get not only their pension but, in some cases, their Aid and Attendance benefits. And they will try to trick them into thinking that they can get you your money faster or get you more benefits. And so it is just so important that we rely on our regulators and organizations like Georgia Watch to provide educational resources and, when we hear about scams, to alert the authorities as quickly as possible so that they are shut down and enforcement happens.

Chairman WARNOCK. Thank you so much, Ms. Coyle.

Ranking Member Tillis.

Senator TILLIS. Thank you, Mr. Chairman, and once again thanks to the witnesses for being here.

Ms. Greszler, the Department of Labor Office of the Inspector General wrote, "The unprecedented infusion of Federal funds into the UI program gave individuals and organized criminal groups a high-value target to exploit. That, combined with easily attainable, stolen, personal, identifiable information and continuing UI program weaknesses identified by the OIG, over the last several years, allowed criminals to defraud the system." Do you agree with that topline assessment?

Ms. GRESZLER. Yes.

Senator TILLIS. Can you explain how the UI system design allowed for both individual and organized criminal elements to exploit it using PII?

Ms. GRESZLER. Yes. And you know, part of it had to do with the nature of the program at the time being outdated, and part of it had to do with all of these expansions that were thrown onto these systems very quickly.

You know, the reason that Government benefit programs will be utilized for criminals to steal money is that, first, an individual's information, which is fairly readily available out there, has to have a value on it. And so what this UI program did is it increased basically the price tag on individuals' personal information.

Prior to the pandemic, maybe you could use somebody's home address and date of birth and name to sell to a telemarketer for a very small sum of money. If you were lucky, then you got credit card information. You could go charge some money on it for a short period of time.

But after the pandemic, you effectively tied $1,000 a week UI benefit to every individual's personal information, and so you are

increasing the price tag and thus attracting more criminals. The more Government benefit programs you have, then more dollar value you tie to those. And unfortunately, a lot of Government benefits programs are targeted toward lower-income individuals. A lot of the ones that are being proposed now would be means-tested or income-limited, and so the criminals go after those populations that have the highest dollar value on them.

But, second, the programs themselves can be a source of compromised information. Some of these State unemployment insurance systems were running non COBOL, which was designed in the 1960s. Universities stopped teaching it in the 1980s. So they were incredibly outdated, and they were not able to adapt quickly. And they did not have the authority like a private company, to say, "Hey, we need to slow things down. We are not going to do this until we know it is safe and we can protect our customers' information." They were required to start delivering the benefits as soon as the legislation was enacted.

Senator TILLIS. Yes, Mr. Chairman, I think this is—one of the reasons why I am highlighting it is I think the storm on the horizon with all these benefits that were fraudulently obtained. I am thinking about households that are going to be completing their taxes next year, or the year after next, and somehow being surprised by the idea that they have received several thousand dollars in taxable benefits, Federal and, where applicable, State taxes.

And then what are they going to have to go through to reconcile it? They may have to hire an attorney. They have got to file a fraud complaint. They could potentially get some concession on not having to pay it, pending the fraud complaint. But I think this is going to be a huge issue that we may have to play a role.

I was trying to sort out this morning how, you know, maybe we can sync up the Department of Labor system, which administered the UI benefit, and banking, which could potentially swim into our—or I should say IRS, so that we can try and identify before they get the big surprise a year from now or 2 years from now, if they were subject to an audit and this information somehow intersects.

Ms. Coyle, I want to ask you a question. We are talking about—in your opening Statement, you made a comment about stepping up, providing more tools for prosecution. What advice would you give us on more work that Congress should do in the area of prevention and financial literacy? What more should we be doing on that front?

Ms. COYLE. Thank you. This time I did it. Thank you, Ranking Member Tillis, for that question. You know, the conversation that has been about theft of benefits is certainly one that we are concerned about. I can tell you that in June I heard from a Georgia consumer whose identity was stolen and found—and used to apply for unemployment benefits. And he had an incredibly difficult time navigating the system of having this issue resolved. So the more we can help the States untangle some of those challenges that are in place, to make sure that those Georgians needing help when they have been scammed, or when their identity has been stolen, would be one of the primary recommendations I would make.

Senator TILLIS. Thank you. Thank you, Mr. Chair.

Chairman WARNOCK. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, Mr. Chair and Ranking Member. Thank you to the panelists.

Let me just start by saying I agree with Senator Tillis. I, listen, as a former attorney general, dealt with fraud and identity theft. And they are interconnected, and it is a reality, and we have not done anything to address really the rampant identity theft.

But I agree with him that we have to put additional resources into the enforcement mechanism against fraud for the IRS as well as Labor, wherever we can, and we have the ability to do that. We have done that in the past. And I think it is going to be important for us to continue, as we look at providing essential resources to individuals, to guard against the predatory nature of fraud which is going to happen.

And so my question to—let me start with Ms. Coyle and to all the panelists. Really, what we are talking about, the essential piece of all of the fraud, is the identity theft that is associated with it.

And, Ms. Coyle, let me start with you. What can be done to address identity theft and/or educate the consumer so that they can guard their personal information or protect against identity theft? Is it too late, or are there things that the individual consumer can do? And let me start with Ms. Coyle, and I will go down the panel, if you——

Ms. COYLE. I sent a message to Mr. Moffat, who is providing technical support. I can—I am unmuted, but unfortunately I was not able to hear that last question directed to me. May I ask that you repeat it? And I hope I will be able to hear it this time, and perhaps Mr. Moffat can fix the technology on his end.

Senator CORTEZ MASTO. Yes, not a problem. Let me then start with Mr. Breyault.

Ms. COYLE. I am sorry I am not able to hear your sound.

Senator CORTEZ MASTO. No, that is not a problem. I am just asking a question. Yes, I am asking the question about——

Ms. COYLE. I am hoping Mr. Moffat can help.

Senator CORTEZ MASTO. Can you hear me now?

[Technical difficulties.]

Senator CORTEZ MASTO. For the sake of the time, let me just then go to Mr. Breyault. The question, same question, with respect to identity theft, is it too late, or are there things that we should be doing or can be doing that consumers can use to guard against, to protect themselves?

Mr. BREYAULT. Yes, Senator. Certainly, the information the information that identity thieves need to defraud millions of consumers is readily available on the dark web thanks to the number of data breaches that Senator Tillis alluded to earlier. What can be done is to do things like better data security standards so that the supply of information from banks and other institutions that hold sensitive personal information is cutoff, so it is harder for the scammers to get it in the first place.

Other things that can be done is to follow the money. Scammers ultimately, end of the day, want to be paid. And so making sure that banks or State UI insurance agencies, who detect this kind of fraud, can claw that money back before it gets lost to the consumers.

And certainly, working with financial institutions who are facilitating the transfer of this money to make sure that they are making security a priority in addition to the speed at which these transactions can be processed. So right now, the Federal Reserve is considering a new money transfer service called FedNow that would allow nearly instantaneous money transfers in competition with the banks' Zelle program. Unfortunately, the regulations that have been put out there for FedNow we and many other consumer advocates do not feel properly prioritize security. And so we are worried that in the name of convenience and speed that the ability of fraudsters to continue to commit identity fraud and ultimately get paid will only become easier.

Senator CORTEZ MASTO. Thank you. I appreciate that.

Ms. Greszler, any thoughts on how we can address the identity theft?

Ms. GRESZLER. Yes. I would just like to add that after somebody actually has the information it is still possible to make it more difficult for them to use that information to obtain Government benefits. And the GAO has identified three sources of improper payments, and while there are some administrative and process errors, the bulk of it comes down to insufficient documentation to determine whether or not somebody is eligible and what the proper amount of the payment should be. And so if you have more documentation and more requirements to actually verify that this is the person that they say they are, that would help. It is going to slow the process down a little bit, but I think that it is still something that is necessary to ensure the integrity of the programs.

Senator CORTEZ MASTO. Thank you. And is there—this is my last question, but I think this is also the challenge that I have found in the past is educating the consumer. To what extent should we be putting resources into educating the consumer to beware of potential scams and how to protect themselves?

Mr. BREYAULT. Senator, consumer education is vital to any fraud prevention program, but as I have said in many other instances, this is a problem that we cannot consumer-educate our way out of. The genie is out of the bottle when it comes to identity fraud. And putting the responsibility on consumers alone to protect their information, when they are fighting back against highly sophisticated, criminal rings of identity thieves, who are often beyond the reach of U.S. law enforcement, is far too much to—a responsibility to put on individual consumers. It has to be an effort that includes banks, that includes software companies, and the Government to try and get a handle on this program.

Senator CORTEZ MASTO. The enforcement is key.

Mr. BREYAULT. Yes, ma'am.

Senator CORTEZ MASTO. Thank you.

Chairman WARNOCK. Ms. Cortez Masto, we had a technology glitch. If you need more time?

Senator CORTEZ MASTO. No.

Chairman WARNOCK. OK. Senator Tester.

Senator TESTER. Thank you, Mr. Chairman and Ranking Member. I am Chairman of the Veterans Affairs Committee. Senator Tillis sits on that Committee. I am interested in how we are protecting the men and women who have protected us. And so this is

question is for you, Mr. Breyault, and that is: How has fraud during the pandemic and economic crisis impacted our veterans?

Mr. BREYAULT. Senator Tester, thank—is my mic on?

Senator TESTER. Yes.

Mr. BREYAULT. Senator, thank you for the question. Members of the military, their families, and others in the military community are uniquely vulnerable to fraud because of the nature of their job. They have a guaranteed income stream. They are often moving around, on a frequent basis, as they move from posting to posting. They are often targeted by fraudsters.

And so the solutions that try and better protect them have to be unique, and those solutions have to come from not only within the Department of Defense, to give these military servicemembers the resources they need to spot and avoid these scams in the first place, but it also have to come from enforcement agencies, like the Department of Justice, the Federal Trade Commission, and banking regulators to crack down on predatory lenders who may target them, on fraudulent direct sellers who may target military families, or other fraudsters who are specifically trying to take advantage of the unique nature of members of the military community.

Senator TESTER. So you are talking about active military. I am talking about the folks who went from active military to the civilian life, that are now civilians or veterans because they have served our military. Are the same challenges—the same solutions to their challenges the same as active military?

Mr. BREYAULT. Well, I think military veterans are certainly deserving of special attention when it comes to fraud protection. As with active military, military veterans often have a guaranteed income stream.

Senator TESTER. True.

Mr. BREYAULT. And that makes them very attractive to scammers. So, yes, I do believe they deserve special attention.

Senator TESTER. So the question becomes: As these scammers that are out there stealing information and using it in a way that deprives people who need the benefits that are out there for them, whether it is unemployment insurance or whether that is in benefits that they get through a disability, so how do we protect them? I mean, how do we actually get to the bottom of this? Is this an issue?

The lady who is here in person talked about old computer systems. And, look, computer systems in the 1960s probably should have been replaced 30 years ago, but the truth is: What do we need to do? Where do we need to put our focus?

Mr. BREYAULT. Senator, I wish there was one silver bullet that could address this bullet, but there just is not. There needs to be a layered approach to better protecting consumers, including veterans, from identity fraud. And that is going to require work by credit reporting bureaus——

Senator TESTER. OK.

Mr. BREYAULT ——by banks, by software companies, by State unemployment insurance programs to update their technology. It is something that is going to take a long time and is going to require investment at all of those levels that I just described.

Senator TESTER. OK. Ms. Coyle, can you hear me?

She cannot. Well, then there is no need asking her any questions.

We are going to go over to the testimony. Let me get your name because I do not want to botch it up too bad. It is not so bad. Ms. Greszler, OK? In your testimony, you talked about—and you talked about this in your opening Statement, too—that there is about 557 million checks that were not actually employed; 807 million went to people who were actually employed and 557 million did not. Those are pretty stark statistics. How confident are you that those are correct?

Ms. GRESZLER. Well, what I did is to tabulate the entire number of checks that went out and then to tabulate the entire number of weeks that people were actually unemployed. You know, traditionally, about 40 percent of people who are unemployed will collect an unemployment insurance benefit.

And so what I said is, well, what if actually 100 percent? If the programs perfectly got everybody that was unemployed and they all got a check, what would that total be? And that is where you have the 807 million benefit checks would have gone out if you were simply covering 100 percent. And so the excess above that is 557 million.

Now because we do not have a match to see those——

Senator TESTER. Yes, I got you.

Ms. GRESZLER ——we do not know exactly. But it is kind of a conservative estimate, to say, that these people were not unemployed and they were receiving benefits.

Senator TESTER. So have you been able to do any research to determine how much of that 557 million was collected by organized crime or organized criminals, however you want to put it, versus people who are just crooked and applied for unemployment benefits when they were not unemployed?

Ms. GRESZLER. I think given the magnitude of it—and you know, the company ID.me that is working with some of the States to increase their fraud protection has estimated it is a $400 billion sum. Given how large that is, I think the overwhelming majority of this is criminal activity as opposed to just individual-level fraud and abuse.

Senator TESTER. OK. I appreciate that. Thank you very, very much.

Chairman WARNOCK. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman. This is a very important Subcommittee, and I am glad to be part of it under your leadership.

So I would like to talk today with you all about mobile apps. You know, these allow people to instantaneously transfer money to friends or family or merchants with just a few taps on their phone. They have proved to be a valuable resource in our socially distanced, pandemic economy, but along with the benefits of instant and contactless payments, these apps have made it easier for scammers and fraudsters to reach more people faster.

A recent report using data from the CFPB shows that consumer complaints about digital payment apps steadily increased over the last few years before skyrocketing during the pandemic. The number of consumer complaints about these apps increased more than 300 percent in just the first 4 months of the pandemic, reached a

peak in April of this year at nearly double the previous high back in 2020.

So, Mr. Breyault, I see you nodding as we go through this. Your organization has done a lot of good work to protect consumers from scams and fraud and abuse, including the scams that they face on mobile apps. So I just want to ask you, when a consumer wants to use their Venmo or Cash App account to pay a friend for lunch, but they make a mistake, say by sending the money to another person who happens to have the same name as their friend, are they usually able to get the money back?

Mr. BREYAULT. No, Senator.

Senator WARREN. Yes. In fact, I understand that if you go to Venmo's help center to figure out what to do when you have been paying the wrong person, the first thing it tells you is ask the person you accidentally paid to send the money back. And if that person is not very nice, I take it you are just kind of out of luck.

Mr. BREYAULT. Yes, that is correct, Senator.

Senator WARREN. All right. So let us just push this a little further, Mr. Breyault. Let us say a consumer is tricked into sending money to someone who pretends to be a coworker collecting money for a gift or to a scammer who promises to flip that money into a bigger payday but never makes good on the deal. In your experience, are consumers likely to get their money back then?

Mr. BREYAULT. No, Senator, they are not.

Senator WARREN. So money in these accounts are more like cash in your wallet than like money in a bank account. Once it is gone, I take it is probably gone for good. Not only does that leave consumers extremely vulnerable to scam artists and to fraudsters, it also leaves them vulnerable to being hounded by the apps themselves. Venmo has deployed predatory debt collection tactics against consumers whose accounts have been drained into the red by scammers, and it has not let up during the pandemic.

So, Mr. Breyault, do you believe that mobile peer-to-peer payment apps should face greater scrutiny from regulators to ensure that they provide consumers with stronger protections against scam and fraud and, frankly, even simple mistakes?

Mr. BREYAULT. Yes, Senator, I do. And I have detailed a number of the steps that this Committee can take to better protect those consumers in my written testimony.

Senator WARREN. Yes. And thank you for that testimony and for the suggestions. You know, I agree with you on this, and that is why I am very glad to see that the CFPB has begun taking steps to strengthen and to clarify consumer protection rules for payment apps.

These apps are helping to fill gaps in a payment system that is too slow; it is too expensive, and it is too inconvenient. And there is no doubt that these apps have played an important role in our pandemic economy. But we cannot leave consumers to fend for themselves on a level playing field that is making it even easier for scammers and fraudsters to use these apps to do harm. That means that if we really do want to level the playing field we have got to make the rules stronger and we have got to make sure there is adequate enforcement, to ensure that mobile payment apps take responsibility for protecting their customers.

I want to say thank you, Mr. Chairman, for holding this hearing, giving us a chance to look at this and so many other aspects of where fraudsters have figured out pandemic is a good time for them to make money and to step up their efforts to cheat everyone else. I look forward to our continuing to work on this, and I look forward to your next hearing.

Chairman WARNOCK. Thank you so much, Senator Warren, for your work in this area for such a long time.

I see that Senator Van Hollen is present and just in time to ask your question.

Senator VAN HOLLEN. Well, thank you, Mr. Chairman, Ranking Member Tillis, for conducting this hearing. I thank all of you for your testimony. And, Ms. Coyle, thank you for all the work that you do in Georgia.

I have a question related to medical debt because on this Committee, you know, we have learned over the years that many Americans are burdened by all sorts of debt. We obviously have student loan debt, household debt. The debt that is most under collection and most responsible for personal bankruptcies continues to be medical debt. Despite improvements many of us think we have made in the health care system and affordability, we have a long, long way to go on that front, but in the meantime, we have people who are being just buried with medical debt.

And so my question is—I do not know if Ms. Coyle is remote, but is, what are you doing in Georgia, because my understanding is that you have some programs underway to try to address this. So what are you doing, but what is the longer-term solution based on your experience?

Ms. COYLE. Thank you, Senator, so much for that question, for your work in this space. Right now in Georgia, some 30 percent of adults have medical debt and 48 percent lack access to a rainy day fund. It is those emergencies, whether it is an unexpected, surprise medical bill, which thanks to hard work in our legislature over a few years we now have a ban on surprise billing in Georgia. But people do not have that even $500 saved up if they have another problem, a very high utility bill or a car that need repaired.

And so with medical—with medical debt, we have put together a comprehensive guide, and Georgians call us for advice all the time. It is our number one call to our consumer hotline. We know that medical debt is actually a barrier to health care itself. We know that because of the fear of the potential cost of a procedure, and the lack of transparency about what a procedure might cost, many people forego getting needed care until they are even sicker and the care will be even more costly.

In Georgia, we have not yet expanded Medicaid, and we do know that the number of uninsured in Georgia as of 2019 is over 13 percent.

Medical debt puts an incredible strain on people's financial health. Thirty-seven percent of people with medical bills' issues used up all their savings to pay for those bills. We call on our health systems, our hospitals, and health care providers to be much more transparent and up-front about offering financial assistance. Many of the Georgians and Americans trapped in medical debt are being hounded by hospitals or other—or third-party debt collectors,

and those same individuals would have qualified for financial assistance if it had been offered. So we want to see much more robust spending in that space and a much better job of working with consumers to offer payment plans and to make sure that the cost of care is transparent and that we do everything we can to ensure, as we do, that people know where they can get free and reduced care. Thank you for that question.

Senator VAN HOLLEN. Well, thank you for what you are doing. Senator Chris Murphy and I and others have introduced legislation during this pandemic to, at least on an emergency basis, you know, prevent some of the debt collectors, some of these worst practices from being implemented because people are being chased down even as they are experiencing other hardships.

But clearly, we need a long-term solution. Part of it is, of course, more affordable health care, but there are other things we can be doing here. I do not know about some of my colleagues. We have a number of churches and other faith-based institutions in our State, who are raising money and paying off people's medical debt. That is a great and kind thing for them to do, and I applaud them for doing, but we should not have a health care system that depends on, you know, people passing a hat at services as the primary mechanism to keep people from experiencing bankruptcy.

And as we see from the figures, despite all their efforts, there is still lots of people who are going into personal bankruptcy and then losing their homes and other things.

So I hope that we will find a way to address this because, as you pointed out, Ms. Coyle, so many times it is like, well, you have this hospital bill, and you are—you know, someone hit the back of your car. You have got to replace your fender. You have got to spend $400 on a car breaking down or whatever it may be, and then you do not pay your medical debt. Then you get hounded. Then you get a bad credit rating. And then you have this cycle. And since medical debt is the number one cause of personal bankruptcy, I really hope we will take a look at it.

Thank you, Mr. Chairman and Ranking Member, and thank all the witnesses.

Chairman WARNOCK. Thank you very much, Senator Van Hollen. And with that, all questioning is concluded.

Thanks again to our witnesses for taking the time to be with us today and to provide your testimony.

Today's hearing on frauds and scams is an important step toward protecting consumers during the pandemic recovery economy, and I look forward to working with my colleagues on both sides of the aisle on this issue. And as I said at the outset, this topic is about helping American families and ensuring that they are not swindled out of their hard-earned dollars.

For Senators who wish to submit questions for the record, those questions are due 1 week from today, on Tuesday, August 10th. And for our witnesses, you have 45 days to respond to any questions. Thank you again. And with that, this hearing is adjourned.

[Whereupon, at 3:41 p.m., the hearing was adjourned.]

[Prepared statements and responses to written questions supplied for the record follow:]

PREPARED STATEMENT OF LIZ COYLE

EXECUTIVE DIRECTOR, GEORGIA WATCH

AUGUST 3, 2021

Good afternoon. Thank you Chairman Warnock and Ranking Member Tillis for inviting me to speak before this Subcommittee today. I am truly honored to have this opportunity.

As Members of this Subcommittee know, our country still is facing significant health risks tied to COVID–19, and recovery from the pandemic economy remains challenging for many and fraught with obstacles and dangers for the most vulnerable among us. Today, we're here to talk about protecting consumers from scams and fraud in the pandemic recovery economy. I am grateful to the Subcommittee for shining a light on this issue.

I would like to share with you today some of my concerns as a consumer advocate from Georgia. Every day, we work to help Georgians with the issues that impact their lives and livelihoods. The pandemic public health and economic crises further highlighted what we already knew. Those already struggling to access needed health care, keep the lights on, pay off debts, and live in stable housing would be much more significantly impacted by the challenges suddenly confronting all of us. Our toll-free consumer hotline started ringing on day one of this crisis and we continue to hear regularly from people needing assistance. This especially is the case among our seniors on fixed incomes, veterans, lower income households and communities of color, who long have been disparately impacted in times of crisis. We knew many consumers in Georgia were feeling desperate and vulnerable. Bad actors definitely knew that, too. From the early days, scammers and fraudsters plotted to benefit substantially from these conditions. And as we've learned from Federal and State regulators, they did.

While many of today's scams look a lot like yesterday's, a newer kid on the economic block may be having an outsized influence on the current shape of fraud. Emerging financial technology tools certainly offer convenience, and for some under- or unbanked Americans, access to the mainstream economy. However, these fintech offerings may also be used by bad actors to facilitate scam-based theft. For example, a mobile lending technology developed by a company from Georgia has been used by home repair scammers as the perfect vehicle to steal from unsuspecting, vulnerable homeowners.

We also have heard from consumers who've been scammed when using a common social media platform, Facebook. Scammers use Facebook to steal money from unsuspecting consumers. Someone might see an ad while using the platform and be tricked into purchasing a product from a fake company. When the merchandise doesn't come, they're left with nothing more than a web address and maybe an email address to a fraudulent, nonexistent company.

In closing these remarks, I want to acknowledge the vitally important role played by the Georgia Attorney General and Department of Law and the Consumer Financial Protection Bureau in alerting us to emerging scams. Notably, these regulators both launched investigations and initiated enforcement actions related to the home improvement scams I just referenced. I recommend policy makers ensure our State and Federal regulators have the authority they need to set and enforce rules that protect consumers and keep the emerging fintech marketplace safe for all. Thank you again.

PREPARED STATEMENT OF JOHN BREYAULT

VICE PRESIDENT OF PUBLIC POLICY, TELECOMMUNICATIONS, AND FRAUD, NATIONAL CONSUMERS LEAGUE

AUGUST 3, 2021

Summary

The COVID–19 pandemic has been a boom time for scammers and a nightmare for their victims. By almost any measure, rates of fraud related to the pandemic have mushroomed. In 2020, the Federal Trade Commission received more fraud complaints than at any time in its 106-year history. The House Select Subcommittee on the Coronavirus Crisis estimates that potential fraud involving the Small Business Administration's Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) programs could cost taxpayers $84 billion. The impact of this fraud has fallen disproportionately on historically marginalized communities, already suffering from high rates of COVID-related illnesses, deaths, and economic hardship.

We are pleased to contribute to the Subcommittee's examination of the role that insecure peer-to-peer (P2P) payment platforms are playing in the transfer of funds from fraud victims to scammers during the pandemic. Unfortunately, the same features that are fueling these services' explosive growth—low cost, nearly instantaneous payments made via a mobile app—have made P2P an increasingly popular payment method for scammers. Analysts estimate that fraud rates on these platforms are three to four times higher than for traditional payment methods such as debit and credit cards.

The lack of consumer protections for victims is a significant reason why fraud rates are so high. Scammers are unlikely to abandon P2P platforms as long as they can be used to easily obtain fraudulent payments. To address this, we recommend that Congress consider extending existing limited liability protections for debit and credit card transactions to cover fraudulently induced payments, requiring more stringent investigations of potentially fraudulent transactions, pushing regulators to enforce error resolution responsibilities for consumer errors and fraudulently induced payments, and mandating more responsive customer service by P2P platforms.

Introduction

The National Consumers League appreciates the opportunity to provide the Subcommittee with our views on protecting consumers from financial fraud and scams as America begins to emerge from the COVID–19 pandemic.

Founded in 1899, the National Consumers League (NCL) is the Nation's pioneering consumer and worker advocacy organization. Our nonprofit mission is to advocate on behalf of consumers and workers in the United States and abroad.[1] For more than 20 years, NCL has worked, via our Fraud.org campaign, to educate consumers about the warning signs of fraud and promote public policies that protect the American public from scams of all kinds.

The COVID–19 Pandemic Has Been a Perfect Storm for Fraudsters

The last 16 months have been boom times for scammers and a nightmare for their victims. To put this in context, in 2020 the Federal Trade Commission (FTC) received 4.72 million complaints from consumers, a 45.7 percent increase over 2019 and by far the largest year-over-year increase in the FTC's history.[2] The median loss reported by victims of these scams was $374, though many victims lost far more. A consumer who contacted NCL's Fraud.org campaign lost $15,000 to a scammer.[3] What is clear is that even these sobering numbers are only the tip of a gigantic iceberg when it comes to COVID-linked fraud.

For example, the Department of Labor recently estimated that one type of fraud alone—unemployment insurance fraud—will have cost taxpayers more than $87 billion over the course of the pandemic.[4] Other estimates have put the amount of unemployment fraud during the pandemic as high as $400 billion.[5] Fraudsters are having a heyday. One Bronx man received $1.5 million in 10 months, a California real estate broker stole more than $500,000 over 6 months, and a Nigerian Government official was recently accused of fraudulently obtaining over $350,000 in less than 6 weeks.[6] Even high-profile politicians are not immune. The personal information of Senator Diane Feinstein[7] and Ohio Governor Mike DeWine[8] was reportedly used by unemployment insurance fraudsters to try and improperly obtain benefits.

---

[1] For more information, visit *www.nclnet.org.*

[2] Federal Trade Commission. "Consumer Sentinel Data Book 2020". February 2021. P. 6. Online: *https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn-annual-data-book-2020.pdf.*

[3] Fraud.org. "Cash App Scams on the Rise", June 1, 2021. Online: *https://fraud.org/cash-app-alert/.*

[4] United States Department of Labor Office of Inspector General. "DOL–OIG Oversight of the Unemployment Insurance Program", June 10, 2021. Online: *https://www.oig.dol.gov/doloiguioversightwork.htm.*

[5] Salmon, Felix. "Half of the Pandemic's Unemployment Money May Have Been Stolen", *Axios.* June 10, 2021. Online: *https://www.axios.com/pandemic-unemployment-fraud-benefits-stolen-a937ad9d-0973-4aad-814f-4ca47b72f67f.html.*

[6] Podkul, Cezary. "How Unemployment Insurance Fraud Exploded During the Pandemic", *ProPublica.* July 26, 2021. Online: *https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.*

[7] White, Jeremy. "Californian Allegedly Obtained UI Benefits Using Feinstein's Identity", *Politico.* December 17, 2020. Online: *https://www.politico.com/states/california/story/2020/12/17/californian-allegedly-obtained-ui-benefits-using-feinsteins-identity-1348423.*

[8] Bischoff, Laura. "Unemployment Fraud So 'Widespread' It Even Happened to DeWine and Husted", *Dayton Daily News.* January 19, 2021. Online: *https://daytondailynews.com/local/unemployment-fraud-so-widespread-it-even-happened-to-dewine-and-husted/XRDFXUC7EFHKVD2C54SEJGFCCQ/.*

The statistics are equally sobering for fraud involving other pandemic relief programs. A recent analysis by the House of Representatives' Select Subcommittee on the Coronavirus Crisis identified nearly $84 billion in potential fraud involving the Small Business Administration's Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) programs.[9]

The variety of scams linked to COVID–19 is staggering. Fraudsters have run advance fee scams targeting consumers' stimulus checks.[10] They have committed identity fraud linked to the sharing of COVID–19 vaccination cards online.[11] Imposter scams have preyed on consumers' fears about Federal Deposit Insurance Corporation-backed bank accounts.[12] Scammers even taken advantage of grieving families by targeting the Federal Emergency Management Agency's COVID–19 Funeral Assistance Program.[13]

The Department of Justice and other enforcement agencies have done yeoman's work to try and crack down on this wave of criminality, particularly scams targeting taxpayer-funded COVID–19 relief programs.[14] Unfortunately, given the scale of fraud linked to the pandemic, these efforts are likely to be little more than temporary setbacks for the armies of sophisticated and well-organized criminal rings.

Many factors have contributed to the historic increase in fraud during the pandemic. Rampant misinformation and disinformation about the virus have been fertile ground for scammers peddling all manner of COVID-prevention pills, testing kits, and treatments. Unprecedented economic distress has created ample opportunities for scammers to run imposter schemes threatening dire consequences if payments aren't made. Scammers can easily contact victims over the phone, text message, email, or over the Web, putting millions of potential victims at their fingertips. These transactions happen with speed and anonymity through gift cards, peer-to-peer (P2P) payment apps, cryptocurrencies, and other money transfer services. Cashing out is easy and relatively risk-free for the criminals.

Taken together, these factors have created a perfect storm of fraud during the pandemic.

The Impact of Fraud Linked to COVID–19 Has Fallen Disproportionately on Marginalized Communities

Consumers' vulnerability to fraud increases during times of economic uncertainty. The COVID–19 pandemic has been no exception. High unemployment, the threat of eviction, and social isolation brought on by social distancing measures have all contributed to high rates of fraud.

While fraud affects consumers of all races, ages, and income levels, consumers from historically marginalized communities have been at particular risk of scams. According to a 2017 FTC survey, 19.2 percent of African Americans and 17.3 percent of Hispanic consumers reported being a victim of fraud compared to 15.9 percent of consumers overall and 14.9 percent of non-Hispanic Whites.[15] The same survey found that 20.4 percent of consumers who have experienced a serious negative life event (e.g., death of a family member or close friend, a serious injury or illness in the family, or the loss of a job) reported being victims of fraud, compared to 13.1 percent of consumers who had not experienced such an event.[16]

---

[9] House Select Subcommittee on the Coronavirus Crisis. "Lowering the Guardrails: How the Trump Administration Failed To Prevent Billions in Pandemic Small Business Fraud", March 25, 2021. Online: *https://coronavirus.house.gov/sites/democrats.coronavirus.house.gov/files/2020-03-25-Staff-Memo-Small-Business-Fraud.pdf.*

[10] Leonhardt, Megan. "5 Common Stimulus Check Scams Experts Are Warning Consumers To Watch For", CNBC.com. December 29, 2020. Online: *https://www.cnbc.com/2020/12/29/stimulus-check-scams-here-are-red-flags-to-watch-for.html.*

[11] Gressin, Seena. "Social Media Is No Place for COVID–19 Vaccination Cards", Federal Trade Commission. February 5, 2021. Online: *https://www.consumer.ftc.gov/blog/2021/02/social-media-no-place-covid-19-vaccination-cards.*

[12] Federal Deposit Insurance Corporation. "FDIC: Insured Bank Deposits Are Safe: Beware of Potential Scams Using the Agency's Name". Press Release. March 18, 2020. Online: *https://www.fdic.gov/news/press-releases/2020/pr20032.html.*

[13] Gressin, Seena. "Scammers Target Loved Ones of COVID–19 Victims". MilitaryConsumer.gov. April 20, 2021. Online: *https://www.militaryconsumer.gov/blog/scammers-target-loved-ones-covid-19-victims.*

[14] United States Department of Justice. "Justice Department Takes Action Against COVID–19 Fraud". Press release. March 26, 2021. Online: *https://www.justice.gov/opa/pr/justice-department-takes-action-against-covid-19-fraud.*

[15] Anderson, Keith. "Mass-Market Consumer Fraud in the United States: A 2017 Update". (Staff Report of the Bureau of Economics, Federal Trade Commission.) Table 11. October 2019. Online: *https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf.*

[16] Ibid. P. 106.

Specific data on the intersection of COVID–19 fraud and minorities is lacking. However, given what we know about the vulnerability of consumers of color to fraud and the high toll that COVID–19 has taken on their communities in terms of deaths, illnesses, and economic harm,[17] we can conclude that fraud linked to the pandemic is taking a similarly disproportionate toll on historically marginalized consumers.

Anecdotal evidence supports this conclusion. This spring, the FTC and the State of Arkansas sued the operators of a "blessing loom" pyramid scheme that allegedly targeted African Americans struggling financially during the pandemic. According to the FTC, the scammers behind the scheme defrauded thousands of consumers of tens of millions of dollars by promising investment returns as high as 800 percent.[18] The National Caucus and Center on Black Aging has also reported an increase in fraud cases targeting cash-strapped or unemployed older African Americans since the pandemic began.[19]

Scammers Are Exploiting a Lack of Protections for Payments Made via Peer-to-Peer Services

The ultimate goal for fraudsters is stealing money. This can take the form of direct payments from the victims to the scammers or stealing information that can then be used to obtain money through identity fraud or other schemes. Scammers routinely take advantage of new financial technologies to facilitate the transfer of funds. While no financial institution wants to be used as a vehicle for crime, there is often tension between businesses' desire to secure a particular payment vector from fraud while still allowing for legitimate transactions to be processed quickly.

This tension is clear when it comes to the rapid growth of P2P payment platforms such as PayPal's Friends & Family and Venmo services, Square's Cash App, and Zelle, which is owned by a consortium of major banks. These services have attracted tens millions of users by allowing for free or very low-cost payments to be sent between consumers or from consumers to businesses.[20] Even before the pandemic, roughly 4 in 5 Americans (79 percent) has used mobile payment apps, by one estimate.[21] Social distancing regulations put in place during the pandemic have supercharged consumers' embrace of these services, with the volume of payments expected to grow by roughly 37 percent in 2021.[22] The explosive growth of these services is not expected to end any time soon. By 2023, it is estimated that more than $1 trillion will be transacted via P2P platforms.[23]

Unfortunately, the same factors that are fueling the rapid growth of P2P payment platforms during the pandemic—low-cost, nearly instantaneous payments made via a mobile app—have made P2P a payment method of choice for scammers. In 2020, the FTC received nearly 62,000 complaints from consumers who sent money to fraudsters via payment apps or similar services, with a total reported loss of $87 million.[24] Consumer complaints to the Consumer Financial Protection Bureau (CFPB or Bureau) tell a similar story. A recent MASSPIRG Education Fund analysis found that more than 5,200 complaints about mobile or digital wallets were filed with CFPB over the 12-month period preceding April 2021. Three companies—PayPal (which owns Venmo), Square (which owns Cash App), and Coinbase (a platform for buying and selling cryptocurrency)—accounted for more than two-thirds of

---

[17] Zamarripa, Ryan, and Roque, Lorena. "Latinos Face Disproportionate Health and Economic Impacts From COVID–19". Center for American Progress. March 5, 2021. Online: *https://www.americanprogress.org/issues/economy/reports/2021/03/05/496733/latinos-face-disproportionate-health-economic-impacts-covid-19/*.

[18] Federal Trade Commission. "FTC and the State of Arkansas Charge Operators of 'Blessing Loom' With Running an Illegal Pyramid Scheme". Press release. June 17, 2021. Online: *https://www.ftc.gov/news-events/press-releases/2021/06/ftc-state-arkansas-charge-operators-blessing-loom-running-illegal.*

[19] NAACP. "Elder Abuse: Another COVID–19 Evil", March 1, 2021. Online: *https://naacp.org/articles/elder-abuse-another-covid-19-evil.*

[20] Kunst, Alexander. "Statista Global Consumer Survey". November 19, 2020. Online: *https://www.statista.com/forecasts/997123/peer-to-peer-payments-in-the-us.*

[21] El Issa. "Most Americans Go Mobile With Payment Apps—Here's How They Roll", NerdWallet.com. February 26, 2020. Online: *https://www.nerdwallet.com/article/banking/mobile-payment-app-survey.*

[22] Ho, Justin. "P2P Payment Apps Are Booming, Thanks to the Pandemic", Marketplace.org. March 15, 2021. Online: *https://www.marketplace.org/2021/03/15/p2p-payment-apps-are-booming-thanks-to-the-pandemic/*.

[23] Kats, Rimma. "In 2023, More Than $1 Trillion Will Transact via Mobile P2P Apps", *Insider Intelligence*. April 19, 2021. Online: *https://www.emarketer.com/content/breaking-down-mobile-p2p-payments-biggest-players.*

[24] Federal Trade Commission. "Consumer Sentinel Network Data Book 2020". February 2021. P. 11. Online: *https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn-annual-data-book-2020.pdf.*

all digital wallet complaints to the Bureau through April 2021.[25] The Better Business Bureau has reported a similar increase in complaints involving P2P services.[26]

A complaint NCL received recently from a consumer in Pennsylvania is typical of the experience for far too many consumers who are induced to send money to fraudsters via P2P payment apps. In the process of trying to activate her Cash Card debit card for Square's Cash App service, the consumer's wife was directed to a phishing website where she inadvertently gave a scammer access to her Cash App account. The fraudsters quickly drained more than $5,000 from the consumer's account. When the consumer contacted his bank and Cash App to address the fraud he was told there was nothing that could be done because he his wife had given her permission for the transaction to the scammer.

Another consumer from Massachusetts sent us a similar story last year. She thought she had booked a vacation rental in Provincetown and she was instructed by the "owner" of the property to send a $1,150 deposit via PayPal. When she arrived at the address on the listing, she found that no such property existed. "The neighbor told me he'd heard of many such scams in Provincetown," she wrote.[27] She contacted PayPal twice to dispute the transaction, but was told that there was nothing that could be done to get her money back.

P2P services are aware that fraudsters use their services to obtain funds from their victims. An NCL review found that all of the major P2P platforms make some effort to educate their users about how to avoid scams. However, voluntary disclosures or consumer education alone are not terribly effective by themselves. Despite the platforms' efforts to educate users about the risks of sending money via P2P platforms, more than half of consumers surveyed by AARP incorrectly assumed that their payments would be protected if there is an error or fraud associated with the transaction.[28]

While P2P services do employ technological measures to stop fraudulent transactions, there is a business incentive not to introduce too many security roadblocks in the payment process. This is because P2P payment platforms, and their sky-high valuations,[29] [30] are dependent on maintaining large transaction volumes. P2P platforms' desire to reduce "friction" in the payments experience is in direct tension the need to prevent fraud.[31] Yet if these platforms are making the decision to skew their services towards speed and convenience at the expense of safety and protection, they must take responsibility for those choices.

What is clear is that existing efforts to secure P2P payments are falling far short of what is needed. Major P2P platforms operators like Square, PayPal and Zelle do not publicly disclose their fraud rates. They should be required to do so. Analysts estimate that fraud rates on these platforms are three to four times higher than traditional payment methods such as debit and credit cards.[32] Javelin Strategy and Research recently found that P2P services saw a 733 percent increase in fraud from 2016 to 2019.[33] The popularity of P2P payments during the pandemic is also evi-

---

[25] Mierzwinski, Ed, et al. "Virtual Wallets, Real Complaints". MASSPIRG Education Fund. June 2021. P. 2. Online: *https://masspirg.org/sites/pirg/files/reports/MA-wallets.pdf.*

[26] Zamost, Scott. "Criminals Launder Coronavirus Relief Money, Exploit Victims Through Popular Apps", CNBC.com. November 18, 2020. Online: *https://www.cnbc.com/2020/11/18/criminals-launder-coronavirus-relief-money-exploit-victims-through-popular-apps.html.*

[27] See, e.g., Martin, Sean. "Vacationers Continue To Be Fooled by Rental Scams", *Provincetown Banner*. August 15, 2019. Online: *https://provincetown.wickedlocal.com/news/20190815/vacationers-continue-to-be-fooled-by-rental-scams.*

[28] AARP. "AARP Survey Finds Majority of Americans Using Payment Apps Unaware of Danger Posed by Scammers". Press release. May 12, 2020. Online: *https://press.aarp.org/2020-5-12-AARP-Survey-Finds-Majority-of-Americans-Using-Payment-Apps-Unaware-of-Danger-Posed-by-Scammers.*

[29] Hale, Kori. "Hip-Hop's Role in Square's $40 Billion Cash App Business Success", *Forbes*. September 22, 2020, Online: *https://www.forbes.com/sites/korihale/2020/09/22/hip-hops-role-in-squares-40-billion-cash-app-business-success/?sh=10d7f8ee7489.*

[30] Rudegeair, Peter. "Cash App's Surge During COVID–19 Pandemic Fuels Square Stock", *Wall Street Journal*. September 2, 2020. Online: *https://www.wsj.com/articles/cash-apps-surge-during-covid-19-pandemic-fuels-square-stock-11599039003.*

[31] Doyle, Ciaran. "Removing Friction and Fraud From P2P Payments", IBM RegTech Innovations. December 6, 2018. Online: *https://www.ibm.com/blogs/regtech/removing-friction-and-fraud-from-p2p-payments/.*

[32] Popper, Nathaniel. "When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps", *New York Times*. October 11, 2020. Online: *https://www.nytimes.com/2020/10/11/technology/fraud-payment-apps.html.*

[33] Javelin Strategy and Research. "Identity Fraud Losses Increase 15 Percent as Consumer Out-of-Pocket Costs More Than Double, According to 2020 Identity Fraud Report". Press release. May 13, 2020. Online: *https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double.*

dent from conversations among fraudsters themselves on the Dark Web. In August 2020 alone, analysts noted that Cash App was mentioned more than 10,500 times, an increase of 450 percent from the previous year. Listings mentioning Venmo and Zelle increased by around 50 percent in the same period. [34]

While no financial service is immune from fraud, protections for consumers who lose money to scammers on P2P apps are sorely lacking. When scammers obtain a consumer's bank account information and use it to initiate a preauthorized payment through the ACH system, or obtain debit card information and use it to initiate payment for fraudulent purchases, the consumer typically has limited liability for such transactions, thanks to the Federal Electronic Funds Transfer Act (EFTA), implemented through the Federal Reserve's Regulation E. [35] Similar consumer protections exist for fraudulent credit card transactions exist under the Fair Credit Billing Act (FCBA). [36] Thanks to these measures, consumers are protected, and credit and debit card issuers and participants in the ACH system have strong incentives to implement stringent antifraud countermeasures. The benefits to consumers of these regulatory incentives is clear. Today, it is not uncommon for a credit card holder whose account has been compromised to be notified by her bank before she even notices a fraudulent charge on her statement.

Unfortunately, while P2P platforms are covered by the EFTA, victims of fraud committed via P2P platforms are often unable to take advantage of the protections afforded. A big reason for this is a loophole in the EFTA that excludes payments initiated by the consumer from the protection for unauthorized charges (also known as "fraud in the inducement" or "victim-assisted fraud"). [37] This allows P2P services and banks to avoid liability for payments sent from consumers to scammers, even when such payments are induced by fraud. [38]

The end result of the loophole for fraudulently induced payments made via P2P platforms is that the liability risk for fraud is transferred from P2P platforms and banks to consumers themselves. Yet it is the platforms that have designed systems that encourage this type of fraud and who set the level of fraud they are willing to tolerate. Moreover, institutions are far more able to handle the costs of protecting consumers from small amounts of fraud in the system, whereas a single instance of fraud can be devastating to a consumer. Unfortunately, the only recourse for many victims of fraud committed via P2P platforms is to throw themselves at the mercy of the banks or P2P platforms and beg to be made whole. Unfortunately, thanks to the lack of legal protections, it is far too easy for the banks and P2P platforms to simply tell fraud victims that they are out of luck.

Indeed, another problem is that most financial institutions are taking an unduly narrow view of their error resolution responsibilities under the EFTA. When consumers call to complain about a fraudulently induced payment, or about a mistake such as entering the wrong amount or wrong cell phone number for the recipient, many institutions are refusing to treat that as an error and refusing to investigate or to try to resolve it. Yet there is nothing in the EFTA or Regulation E that excludes consumer errors from the definition of "error." Even if a consumer might ultimately be liable for a payment because it was initiated by the consumer and thus is not "unauthorized," that does not mean that institutions do not have a duty to investigate and try to resolve the matter. A refusal to take these fraud reports and to pass them on to the receiving institution also deprives that institution that holds the scammer's account (or that of a money mule who themselves may be a victim of fraud) of the information needed to put a hold on the funds or shut down that account to prevent further fraud.

Difficulty in obtaining appropriate customer service is especially acute with app-based services that rely on automated communications and do not make live customer service available or adequately staff customer service lines. Problems that consumers have experienced with neo-bank accounts like Chime show the impor-

---

[34] Popper, Nathaniel. "When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps", *New York Times*. October 11, 2020. Online: *https://www.nytimes.com/2020/10/11/technology/fraud-payment-apps.html*.

[35] Federal Deposit Insurance Corporation. "Laws and Regulations: Electronic Funds Transfer Act". February 2019. Online: *https://www.fdic.gov/news/financial-institution-letters/2019/fil19009b.pdf*.

[36] 15 U.S.C. 1666-1666j.

[37] Cornell Law School Legal Information Institute. "Fraud in the Inducement". June 2020. Online: *https://www.law.cornell.edu/wex/fraud-in-the-inducement-Fraud-in-the-inducement-occurs-damages-or-terminate-the-contract*.

[38] Mierzwinski, Ed, et al. "Virtual Wallets, Real Complaints". MASSPIRG Education Fund. June 2021. P. 9. Online: *https://masspirg.org/sites/pirg/files/reports/MA-wallets.pdf*.

tance of making human beings available to address problems when things go wrong. [39]

The Federal Reserve Should Ensure That FedNow Is Safe for Consumers Before the System Is Launched

The Federal Reserve Board (FRB) is in the middle of building a new faster payment system called FedNow, which will be an alternative to Zelle and other private systems. [40] The FRB has recently proposed one set of rules governing the system. [41]

We see the value in the FRB's decision to build a real time payment system. It is imperative, however, that the inadequacies in consumer protection with regards to fraudulent P2P payments not be exacerbated as the FRB continues development of its FedNow service. [42] The rules proposed to date do not address the problems discussed in these comments.

As a public body, the FRB has an especially great responsibility to make sure that a system it designs and runs is safe. Protections in the FedNow system can be a model for other P2P systems. Congress has a critical role to play by insisting that the FRB meets this challenge. Now, during its design phase and before it is deployed to the public, these challenges must be addressed.

New Protections Are Needed To Protect Consumers From Fraud and Errors on P2P Payment Platforms

The lack of consumer protections for users of P2P payment platforms must not be ignored. It is clear from their explosive growth that P2P payment apps are here to stay. It is equally clear that absent regulatory incentives, effective self-regulation by the P2P services will be stymied in the name of protecting transaction volume growth. NCL has spoken with P2P platforms and urged them to offer far more robust fraud protection, but so far we have seen little improvement. The P2P services will continue to rely on marginally effective warnings and disclosures to consumers—an old-fashioned tactic—rather than embracing their responsibility to design systems for safety and using modern artificial intelligence, machine learning, data analytics, and other methods to prevent and remedy fraud.

To ensure that P2P platforms are secure for their users and do not continue to be powerful tools for fraudsters, action by Congress is urgently needed.

Specifically, we urge Congress to:

- Enact legislation to expand the definition of "unauthorized electronic fund transfer" in the Electronic Funds Transfer Act to cover fraudulently induced payments, with ultimate liability resting with the institution that received the fraudulent payment;
- Push regulators to require P2P platforms to investigate errors and fraud, even in cases where the consumer sent a payment erroneously or as a result of fraud in the inducement;
- Urge bank regulators to emphasize fraud prevention and remediation as part of financial institutions' know-your-customer duties;
- Enact legislation to require P2P platforms to prominently display warning about fraudulent use of P2P payments and how to avoid scams;
- Require P2P platforms to provide and prominently display a customer service telephone line and respond to customer service inquiries in a timely manner; and, [43]
- Insist that the Federal Reserve promulgate rules for the design of the FedNow payments service that prioritize safety and security of payments.

---

[39] Kessler, Carson. "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money". *ProPublica*. July 6, 2021. Online: *https://www.propublica.org/article/chime?utm-source=sailthru&utm-medium=email&utm-campaign=dailynewsletter&utm-content=feature.*

[40] Tahyar, Margaret et al. "FedNow: The Federal Reserve's Planned Instant Payments Service", Harvard Law School Forum on Corporate Governance. August 31, 2020. Online: *https://corpgov.law.harvard.edu/2020/08/31/fednow-the-federal-reserves-planned-instant-payments-service/.*

[41] FRS-2021-0214-0001. Online: *https://www.regulations.gov/document/FRS-2021-0214-0001.*

[42] Letter from Americans for Financial Reform Education Fund, et al., to Board of Governors of the Federal Reserve System. November 7, 2019. Online: *https://www.nclc.org/images/pdf/cons-protection/coalition-letter-interbank-settlements.pdf.*

[43] Note: The California legislature is currently considering AB-1320, which contains similar requirements. Online: *https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill-id=202120220AB1320.*

Conclusion

Chairman Warnock, Ranking Member Tillis, and the Members of the Subcommittee, we thank you for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

PREPARED STATEMENT OF RACHEL GRESZLER
RESEARCH FELLOW, THE HERITAGE FOUNDATION
AUGUST 3, 2021

The Heritage Foundation

CONGRESSIONAL TESTIMONY

Protecting Consumers from Financial Fraud and Scams in the Pandemic Recovery Economy

Testimony before the

Subcommittee on Financial Institutions and Consumer Protection

Committee on Banking, Housing, and Urban Affairs

U.S. Senate

August 3, 2021

Rachel Greszler
Research Fellow in Economics, Budgets, and Entitlements
The Heritage Foundation

My name is Rachel Greszler. I am a Research Fellow in Economics, Budgets, and Entitlements at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

The onset of the COVID-19 pandemic led to a tremendous expansion in government programs providing funds to individuals, families, and businesses. Many of these programs helped prevent a deeper and more prolonged crisis by keeping afloat businesses that otherwise would have failed, and by preventing individuals and families from losing their housing or having essential services cut off. But these programs have not been without consequence, including widespread fraud and abuse with individuals' personal identifiable information stolen, as well as significant taxpayer costs and some adverse impacts on the recovery.

In my testimony today, I would first like to discuss the unintended consequence of fraud and abuse in the pandemic unemployment insurance (UI) programs. I will then consider the implications of proposed unemployment insurance expansions and the creation of large new government programs on individuals' privacy and financial security, and on the integrity of taxpayers' dollars.

Unintended Consequences of Pandemic Unemployment Insurance Expansions

Unemployment insurance benefits operate through individual states, which typically provide benefits to workers that equal between 40 percent and 50 percent of their previous wages, for up to 26 weeks. But not all unemployed workers are eligible for unemployment benefits; to qualify, workers must have been in covered employment (meaning that they worked for a traditional employer who paid into the unemployment

insurance system on their behalf), must have been consistently employed for a specified number of months, and typically must have been laid off through no fault of their own (as opposed to quitting or being fired).

In response to the COVID-19 pandemic, which resulted in government-imposed shutdowns of many businesses and tens of millions of workers losing their jobs and incomes through no fault of their own, Congress sought to temporarily expand unemployment benefits to reach more individuals who had lost income. Some of the pandemic unemployment insurance expansions included:[1]

- **Increased benefit levels.** Congress provided an unprecedented $600 weekly supplement to state unemployment insurance benefits from March 2020 through July 2020, and an additional $300 weekly supplement from December 2020 through September 2021. Congress also added an additional $100 per week on top of other unemployment benefits, available from December 2020 through September 2021, to "mixed earners," who had at least $5,000 of self-employment income in the prior year.

  The higher benefit levels attracted more criminals to seek Americans' identities to fraudulently claim unemployment insurance benefits. And the fact that more than two-thirds of unemployed workers were initially receiving more from unemployment benefits than from their previous paychecks undoubtedly prolonged many workers' periods of unemployment.[2]

- **Extended benefits.** Congress extended eligibility for unemployment insurance benefits from the usual 26-week limit (six months) to 79 weeks (18 months).

  Economic studies consistently show that extended benefits lead to longer durations of unemployment.[3] For example, researchers at the Federal Reserve Bank of New York estimated that the extended unemployment benefits during the Great Recession contributed significantly to the long period of high unemployment, increasing the number of unemployed workers by about 4.6 million in 2010 and by 3.3 million in 2011.[4] The extended benefits undoubtedly increased some workers' periods of unemployment and allowed criminals to steal more weeks' worth of unemployment benefits.

- **Expanded coverage, added eligibility criteria, and reduced verification.** Congress established the Pandemic

[1]The goal of the UI expansions did include extending benefits to people who would not traditionally be counted as unemployed, such as parents needing to stay home with children due to school and childcare closures, and workers unable to report to work because of COVID-19 closures. However, other economic policy responses, such as 12 weeks of mandated paid family and medical leave with federally financed tax credits, and the Paycheck Protection Program funds to continue workers' paychecks, provided financial support to these workers outside the UI systems.

[2]Peter Ganong, Pascal J. Noel, and Joseph S. Vavra, "US Unemployment Insurance Replacement Rates During the Pandemic," NBER *Working Paper* No. 27216, May 2020, https://www.nber.org/system/files/working_papers/w27216/w27216.pdf (accessed August 1, 2021).

[3]Drew Gonshorowski and Rachel Greszler, "The Impact of Additional Unemployment Insurance Benefits on Employment and Economic Recovery: How the $600-per-Week Bonus Could Backfire," Heritage Foundation *Backgrounder* No. 3490, April 29, 2020, https://www.heritage.org/sites/default/files/2020-04/BG3490_0.pdf.

[4]Marcus Hagedorn et al., "Unemployment Benefits and Unemployment in the Great Recession: The Role of Equilibrium Effects," The Federal Reserve Bank of New York *Staff Report* No. 646, revised September 2019, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr646.pdf (accessed April 13, 2020).

Unemployment Assistance program to provide benefits—both regular state-level benefits plus the $600 and $300 bonuses—to workers who do not pay into the unemployment insurance systems. This included individuals such the self-employed, freelancers, and gig workers, as well as others who may not have lost a job or income as a result of the pandemic.

In addition to adding coverage for new groups of workers, Congress added new criteria—other than being laid off through no fault of one's own—through which individuals could collect unemployment insurance benefits such as being "impacted" by school or daycare closures, quitting one's job for reasons related to COVID-19, losing partial income, or the very broad qualification of having one's employment be "affected" by COVID-19.

These expansions made it impossible for unemployment insurance programs to utilize their normal verification processes, in which an individual's employer has to verify that they were laid off through no fault of their own. Consequently, most unemployment insurance programs had to rely on self-verification of past income and employment. This opened the door to individual-level fraud and abuse by workers filing for their own benefits, but more significantly, it allowed criminals to file for and receive benefits on behalf of individuals without their knowledge.

While these expansions undoubtedly helped ease the financial consequences for individuals who lost jobs and incomes because of the pandemic, they also had significant unintended consequences. In addition to contributing to the current labor market shortage by making it easier and sometimes more advantageous for individuals to be unemployed than employed, the expansions were also exploited by criminals with total benefit payments far-exceeding policymakers' intent.

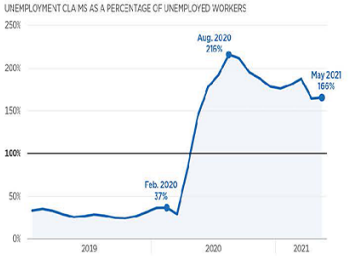
Unemployment Benefits Have Exceeded Unemployed Workers

Typically, about 40 percent of unemployed workers receive unemployment insurance benefits.[5] Since the pandemic began, far more people have received unemployment benefits than have actually been unemployed. Between April 2020 and May 2021, the number of people receiving unemployment benefits averaged 176 percent of the number of unemployed people.[6]

CHART 1

Unemployment Benefits Exceed Unemployed Workers

Historically, about four out of every 10 unemployed workers received unemployment benefits. Since Congress expanded benefits during the COVID-19 pandemic, about 18 workers have received benefits for every 10 unemployed workers.



SOURCE: News release, "Unemployment Insurance Weekly Claims," U.S. Department of Labor, July 1, 2021, https://www.dol.gov/ui/data.pdf (accessed July 7, 2021).

BG3637 heritage.org

[5]There are various reasons why not all unemployed workers collect unemployment benefits, including not participating in the UI system due to self-employment, not having worked long enough to qualify for benefits, or choosing not to file for benefits due to short spells of unemployment.

[6]U.S. Department of Labor, Employment and Training Administration, Office of Unemployment Insurance, "UI Weekly Claims," data archive, https://oui.doleta.gov/unemploy/claims_arch.asp (accessed June 30, 2021).

Between April 2020 and May 2021, the number of continued claims that were processed and paid out totaled 1.365 billion cumulative weeks of benefits. Had the pandemic programs provided unemployment benefits to 100 percent of all unemployed workers, the cumulative number of benefit checks sent out would have been 807 million, which implies that at least 557 million [7] benefit checks went to people who were not actually unemployed. [8] The number of unemployment benefits sent out above and beyond 100 percent of unemployed workers equals about 41 percent of all benefits. Assuming there was no significant difference in the size of benefit claims that went to unemployed workers verses those to people other than unemployed workers, then $357 billion [9] of the estimated $873 billion [10] in total pandemic unemployment insurance benefits did not actually go to unemployed workers. [11] While some states have successfully recovered hundreds of millions, or up to a couple billion dollars, total recoveries will likely pale in comparison to the magnitude of fraud.[12]

[7]Figures do not add due to rounding. The 557 million figure comes from subtracting 807.5 million claims that would have covered 100 percent of unemployed workers' benefits from the 1,364.9 million in claims that were paid out, leaving an excess claims total of 557.4 million.

[8]This analysis compiles all of the weekly continued claims data provided by the Department of Labor's Employment and Training Administration and compares those weekly claims levels to the monthly reported totals of unemployed workers based on the Bureau of Labor Statistics' (BLS's) monthly employment reports. For example, the continued UI claims for June 2020 equaled (in millions of claims): 30.6 + 31.5 + 32.4 + 32.0 = 126.5 total claims, while the number of unemployed people, as measured during the second week of the month, and assumed to hold steady across all four weeks of the month equaled (in millions of workers): 17.7 + 17.7 + 17.7 + 17.7 = 70.8, for a comparison of 126.5 million cumulative weeks of unemployment insurance benefits compared to 70.8 million cumulative weeks of unemployed workers. The unemployment figures reported by the BLS are based on a representative sample of about 60,000 U.S. households. COVID-19 had some impact on the BLS's collection, including lower response rates, which may have resulted in different weightings applied to respondents' surveys. Moreover, beginning in March of 2020, the BLS changed the definition of "unemployed" to include people who were employed but absent from work (such as those not working but still receiving paychecks through the Paycheck Protection Program). Yet, this change was not fully adapted by all surveyors, and some individuals who were still employed but absent from work were counted as employed while others were counted as unemployed. Compared to the pre-COVID-19 definition of unemployment, the official unemployment figures reported (included in this analysis) were higher than they would have been under the old definition, meaning that this analysis does count among the unemployed a portion of workers who were still employed but absent from work for COVID-19-related reasons. For an explanation of the misclassification errors, see Rachel Greszler, "What Policymakers Need to Know About 'Misclassifications' in Recent Unemployment Reports," The Daily Signal, June 16, 2020, https://www.dailysignal.com/2020/06/16/what-policymakers-need-to-know-about-misclassifications-in-recent-unemployment-reports/.

[9]This estimate of $357 billion equals 41 percent of the estimated $873 billion in total pandemic unemployment insurance benefits. Since not all unemployed workers filed for and received UI benefits during every week of unemployment, the 41 percent figure likely represents a lower bound on the percentage of payments that went to unemployed workers.

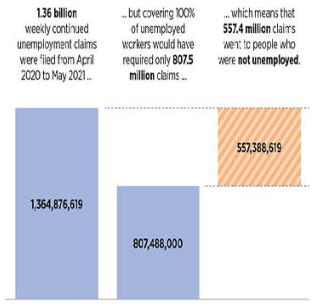
[10]U.S. Department of Labor, Office of Inspector General, "DOL–OIG Oversight of the Unemployment Insurance Program," June 10, 2021, https://www.oig.dol.gov/doloiguioversightwork.htm (accessed June 29, 2021).

[11]While some programs, such as short-time compensation and workshare, provide benefits to workers who are not unemployed but have lost some of their work, these programs accounted for a tiny fraction—about 0.5 percent—of all pandemic unemployment benefits.

[12]News release, "U.S. Secret Service Helps Recover $2B Through Investigations into COVID-19-Related Financial Fraud," U.S. Secret Service Media Relations, May 12, 2021, https://www.secretservice.gov/newsroom/releases/2021/05/us-secret-service-helps-recover-2b-through-investigations-covid-19#:~:text=One%20year%20into%20investigating%20COVID,to%20state%20unemployment%20insurance%20programs (accessed July 6, 2021).

CHART 2

Half a Billion Excess Claims for Unemployment Benefits



SOURCES: News release, "Unemployment Insurance Weekly Claims," U.S. Department of Labor, July 1, 2021, https://www.dol.gov/ui/data.pdf (accessed July 7, 2021), and U.S. Bureau of Labor Statistics, "Civilian Unemployment (Seasonally Adjusted)—LNS12000000," https://data.bls.gov/cgi-bin/surveymost?bls (accessed June 20, 2021)

BG3637 heritage.org

Widespread Fraud, Identity Theft, and Abuse

By putting an unprecedentedly high dollar value on unemployment insurance benefits, making them available for three times as long as usual, widening eligibility, and reducing verification requirements, unemployment insurance benefits were not only abused by some individuals, but they became a high-value, easily accessible target for criminals.

According to the Office of Inspector General (OIG),

> The unprecedented infusion of federal funds into the UI program gave individuals and organized criminal groups a high-value target to exploit. That, combined with easily attainable stolen personally identifiable information and continuing UI program weaknesses identified by the OIG over the last several years, allowed criminals to defraud the system.[13]

The OIG noted that had improper payments throughout the pandemic remained at their usual pre-pandemic 10 percent rate, the federal government would have issued $87 billion in improper payments. (The OIG estimates up to $873 billion in total pandemic unemployment insurance benefits.)[14] The Inspector General report notes, however, that ongoing investigations find that the improper payment rate exceeds 10 percent.[15]

Some researchers have estimated improper payment rates approaching 50 percent within the pandemic unemployment insurance programs. For example, Blake Hall, CEO of the authentication company ID.me, said, "The fraud rates that we're seeing are over 10 times what we usually see at federal agencies."[16] Hall, whose company works with about two dozen states to detect fraudulent benefit claims, estimates that unemployment fraud has potentially cost taxpayers $400 billion. My analysis estimates that $357 billion worth of payments will have gone to non-unemployed individuals.

Unemployment insurance fraud has been so high that the OIG is investigating or reviewing more than 100,000 complaints of fraud, and these unemployment insurance fraud investigations account for 87 percent of the Inspector General's cases, compared to 12 percent prior to the pandemic.[17]

In addition to the cost to taxpayers—which, this author's analysis of $357 billion going to non-unemployed people would consume the

[13]U.S. Department of Labor, Office of Inspector General, "DOL–OIG Oversight of the Unemployment Insurance Program."
[14]Ibid.
[15]Ibid.
[16]Consumer Bob and Nicholas Kjeldgaard, "Unemployment Benefits Fraud Could Cost $300 Billion Nationwide," NBC San Diego, March 24, 2021, https://www.nbcsandiego.com/news/local/unemployment-benefits-fraud-could-cost-300-billion-nationwide/2558796/ (accessed July 6, 2021).
[17]U.S. Department of Labor, Office of Inspector General, "DOL–OIG Oversight of the Unemployment Insurance Program."

entire annual wages of 6.9 million median workers—unemployment expansions have also caused a personal-identity-theft assault on hundreds of thousands—if not millions—of Americans.

In the one-year period prior to the pandemic—between April 2019 and March 2020—the Federal Trade Commission (FTC) received 23,471 identity theft reports from individuals who said their personal information had been used to obtain a government document or claim a government benefit. [18] In the year following the pandemic—from April 2020 to March 2021—the FTC received 636,520 such reports—a 27-fold increase in a single year.[19]

While states have undertaken efforts to detect and prevent fraud, some states' actions may have *fueled* fraud. According to the *Los Angeles Times*, though the California state auditor recommended in March 2019 that the Employment Development Department (EDD) stop including Social Security numbers in its mailed documents, the EDD continued to send out 38 million pieces of mail containing Social Security numbers after the onset of the pandemic.[20] Of the California EDD's estimated 10 percent to 27 percent of fraudulent benefits paid out,[21] 35,000 were issued to names of California prison inmates.[22]

In addition to outright criminal activity through stolen identities, there has almost certainly been a high level of individual misuse, abuse, and fraud. Factors such as self-reported verification of eligibility standards allowed people to lie about whether they were working, to falsify how much income they were receiving prior to the pandemic, and to hide income they earned while receiving unemployment benefits.

Moreover, the generous benefits and easy eligibility undoubtedly caused workers to choose unemployment benefits over work. Anecdotes from employers across the country show this to be the case, and the data also confirm it. Never before has America experienced relatively high unemployment alongside a record number of job openings, a record-high quits rate, and a record-low number of layoffs.[23]

[18]See Tableau Public, "Identity Theft Reports by the Federal Trade Commission," FTC Consumer Sentinel Network Report, https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime (accessed August 2, 2021), and Federal Trade Commission, "Protecting Consumers During the COVID-19 Pandemic: A Year in Review," April 16, 2021, https://www.ftc.gov/system/files/documents/reports/protecting-consumers-during-covid-19-pandemic-year-review/covid_staff_report_final_419_0.pdf (accessed July 6, 2021).

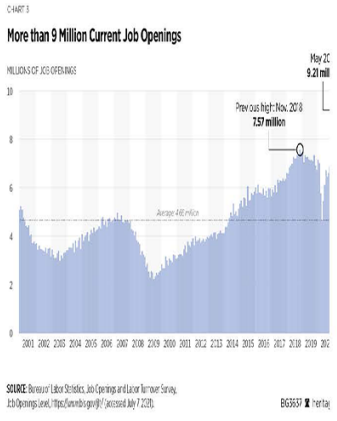
[19]Ibid.

[20]Patrick McGreevy, "Despite Reports of Unemployment Fraud, California Keeps Sending Mail with Social Security Info," *Los Angeles Times*, November 19, 2020, https://www.latimes.com/california/story/2020-11-19/california-edd-unemployment-social-security-numbers-fraud-forms (accessed June 29, 2021).

[21]State of California Employment Development Department, "California Unemployment: Fraud by the Numbers," January 16, 2021, https://www.edd.ca.gov/Unemployment/pdf/fraud-info-sheet.pdf (accessed July 6, 2021).

[22]Jack Kelly, "The Most Brazen $400 Billion Unemployment Funds Heist in History," *Forbes*, June 12, 2020, https://www.forbes.com/sites/jackkelly/2021/06/12/the-most-brazen-400-billion-unemployment-funds-heist-in-history/?sh=b3bbd302020e (accessed July 6, 2021).

[23]Rachel Greszler, "Fact Check: Was Biden Right About Federal Unemployment Benefits Having No Effect on Jobs Report?" The Daily Signal, May 12, 2021, https://www.dailysignal.com/2021/05/12/fact-check-was-biden-right-about-federal-unemployment-benefits-having-no-effect-on-job-report/.



Caution Against Permanent Unemployment Insurance Expansions

Both prior to and since the pandemic, policymakers have introduced proposals to expand the federal government's role in unemployment insurance,[24] including:

- Mandating that states provide at least 26 weeks of benefits, cover at least 75 percent of a typical worker's prior wages, cover part-time workers and those who quit their jobs with good cause, and eliminate one-week waiting periods;
- Establishing programs to cover independent workers, such as the self-employed, freelancers, contractors, and gig-workers;
- Expanding the current federal program to kick in automatically as a supplement based on economic conditions, and to provide 100 percent benefit replacement during major disasters or public health emergencies;
- Establishing a $250 weekly Job Seeker's Allowance available to any unemployed workers not covered by the traditional unemployment insurance system, such as self-employed workers and new entrants into the labor force; and
- Creating a $25 weekly allowance per dependent of unemployed workers.

As the pandemic unemployment programs proved, the higher dollar-value that unemployment benefits carry and the more easily accessible they become, the more readily criminals will steal Americans' identities to claim unemployment benefits. The magnitude of criminal fraud and the sheer number of Americans' identities that have been stolen throughout the pandemic suggest that the primary beneficiaries of such expansions may not be unemployed workers themselves, but rather criminals, with Americans' identities and tax dollars on the line.

Moreover, while these proposals are seemingly well-intended at improving the financial security of workers, government programs are not the most effective means to achieve this goal, and they will inevitably result in unintended consequences and costs.

For starters, economic studies consistently show that higher benefit levels and longer durations lead to higher levels of claims and longer periods of unemployment. As the Congressional Budget Office's analysis of extending the initial $600 bonus payments showed, higher benefit levels would be a drag on medium- and longer-term economic output and growth.[25]

[24]News release, "Bennet, Wyden Unveil Unemployment Insurance Overhaul," Senator Michael Bennet, April 14, 2021, https://www.bennet.senate.gov/public/index.cfm/2021/4/bennet-wyden-unveil-unemployment-insurance-overhaul (accessed June 29, 2021).

[25]Congressional Budget Office, "Economic Effects of Additional Unemployment Benefits of $600 per Week," Letter to the Honorable Charles Grassley, June 4, 2020, https://www.cbo.gov/system/files/2020-06/56387-CBO-Grassley-Letter.pdf (accessed August 1, 2021).

Unemployment insurance programs are effectively a means of forced savings, but with rigid rules and a bureaucratic process required to access the savings. Although employers pay the tax to finance unemployment programs, workers ultimately bear the cost of employment-based taxes through lower wages and benefits. This would cause workers to pay both for the direct expansion in benefits (such as larger unemployment checks and longer durations) and for the resulting increase in unemployment caused by those expansions.

Unemployment Insurance Not Practical, Effective for Independent Workers. Extending benefits to independent workers would be far more complicated and problematic than the existing unemployment insurance programs because these workers are their own bosses. The problems with insuring independent workers include difficulties with verifying past income, the lack of an employer to verify the reason for a claim (it would be hard to distinguish between workers who lost work through no fault of their own and those who wanted to take a month off), and administrative complications, such as the enforcement of a new unemployment insurance tax on millions of independent workers who have variable income and employment.

Moreover, unemployment insurance would be of little or no advantage to independent workers when compared to traditional savings. If workers were to make claims for unemployment insurance benefits, they would face steep unemployment insurance tax rates in the future. Furthermore, while it is common for independent workers to have swings in their income levels, it is less common for them to suddenly lose all income, which is the shock that traditional unemployment insurance programs seek to prevent.

Expanded and New Government Programs Would Open More Doors to Fraud

In addition to expanding unemployment insurance programs, many federal policymakers seek to implement multiple costly new government programs that would send checks to individuals and families and to select businesses that would need to collect, store, and transmit individuals' and children's personal information electronically or through the mail. Each time that an individual has to provide their personal information creates an opportunity for a criminal to steal that individual's identity and use it to receive government benefits, or potentially to sell it to others seeking the identity of an American citizen.

Moreover, the amount of taxpayers' money wasted—through improper payments—is extremely high for federal programs. This is especially true for so-called refundable tax credits, which are effectively just payments associated with having filed taxes without necessarily having worked or paid federal taxes.

A May 2021 report from the Treasury Department's Inspector General for Tax Administration suggests that improper payment rates are not something that policymakers or government agencies can easily reduce, but are inherent to the nature of government programs:

> Although error rates for each of these credits remain high, the IRS attributes these refundable tax credit overclaims to their statutory design and the complexity taxpayers face when self-certifying eligibility for the refundable tax credits and not to internal control

weaknesses, financial management deficiencies, or reporting failures.[26]

Monthly Child Payments Ripe for Fraud and Errors. Already, the Additional Child Tax Credit (which is the refundable portion of the Child Tax Credit) has a 12 percent improper payment rate.[27] Improper payments include erroneous and fraudulent payments.

The now-temporary, but proposed-to-become-permanent, child payments of $250 and $300 per month ($3,000 and $3,600 per year) could be subject to even higher improper payment rates. For starters, the increased amount would entice more people—whether criminals or family members who are not entitled to the payments—to wrongly claim them. By removing the current child tax credit requirement that individuals have reported taxable income to claim the credit, it would be easier for people to falsely claim monthly child payments.

Moreover, the monthly delivery of payments based on individuals' prior years' tax filings could result in payments delivered to the wrong addresses or wrong bank accounts. (If no information is available from the prior tax filing year, payments will be sent based on two-years' prior returns, increasing the risk of errors and fraud.) Families move throughout the year, children in the foster system frequently change homes, there are blended families with children from different parents, many families lack bank accounts, and some even lack homes altogether. Delivering nearly 900 million monthly child payments to the correct place will almost certainly be prone to more errors and fraud than incorporating tax credits for 70 million children into parents' annual tax filings.[28]

At an estimated cost of nearly $1.6 trillion over 10 years, a 12 percent improper payment rate would translate into an additional $187 billion in additional errors and fraud (on top of existing improper payments within the child tax credit).[29] But the higher dollar value, lack of income verification requirements, and monthly payment structure would almost certainly entice greater fraud and cause additional errors. If improper payment rates were to reach the 24 percent and 27 percent that exist, respectively, within the Earned Income Tax Credit and Net Premium Tax Credit (Obamacare subsidies), fraud and improper payments within the expanded portion of monthly child payments would exceed $400 billion over the next 10 years. If improper payments within the existing child tax credits were to have similar improper payment rates when transitioned to monthly payments, the total cost of all improper and fraudulent child payments could exceed $700 billion.[30]

---

[26]Treasury Inspector General for Tax Administration, "Improper Payment Rates for Refundable Tax Credits Remain High," May 10, 2021, https://www.treasury.gov/tigta/auditreports/2021reports/202140036fr.pdf (accessed August 1, 2021).

[27]Ibid.

[28]There were an estimated 74.1 million children ages zero through 17 in the U.S. in 2021. Multiplying this figure by 12 equals 890 million monthly child payments. The current Child Tax Credit excludes 17-year-olds, resulting in roughly 70 million children ages 16 and under in 2021. Child population figures available at: Childstats.gov, "POP1 Child population: Number of children (in millions) ages 0–17 in the United States by age, 1950–2019 and projected 2020–2050," https://www.childstats.gov/americaschildren/tables/pop1.asp (accessed August 1, 2021).

[29]Erica York and Huaqun Li, "Making the Expanded Child Tax Credit Permanent Would Cost Nearly $1.6 Trillion," Tax Foundation, March 19, 2021, https://taxfoundation.org/expanded-child-tax-credit-permanent/ (accessed August 1, 2021).

[30]According to the Congressional Research Service, the total cost of existing Child Tax Credits was $118 billion in 2018. This estimate increases that annual amount in proportion to the child population through 2031, for an estimated total of $1.333 trillion in current-law child tax credits for the period 2022–2031. Added to the Tax Foundation's estimated $1.558 trillion cost of the monthly payment expansion brings the total to $2.891 trillion over 10 years. See Congressional Research

Childcare Subsidies: Potentially High Error Rates, Risk for Children's Identities. President Biden has proposed to spend $225 billion of taxpayers' dollars to provide subsidies for the childcare of virtually all young children in the U.S. It is not entirely clear yet how those subsidies would work, but it could be similar to the Obamacare exchanges, where childcare providers that comply with the federal government's requirements would be listed among a federal childcare exchange network upon which families could shop for childcare.[31]

For starters, childcare payments would likely be subject to significant improper payments as their levels would vary with parents' incomes and the custody arrangements of a child. The Earned Income Tax Credit and Obamacare Subsidies (Net Premium Tax Credits), which respectively have 24 percent and 27 percent improper payment rates, provide a good estimate for the improper payment rates that could come alongside subsidized childcare payments.

Moreover, the subsidies would require a new federal database exchanging information with tens of thousands of child care providers. To receive the subsidies, childcare providers would have to obtain significant personal information from both parents and children, likely including full names, home addresses, cell phone numbers, places of employment, dates of birth, and social security numbers. The storage and transmission of this information across providers and the federal government would open the door to criminals stealing personal information that they could use for any number of purposes, such as claiming monthly child payments, filing unemployment insurance claims on behalf of parents, or selling personal information to third parties or to individuals in search of a U.S. citizen's identity.

Government Paid Family Leave Another Privacy and Fraud Concern. Among the many other government programs the Biden Administration seeks to establish is a federal paid family leave program. Unlike receiving paid family leave through an employer—who already has the individual's information and does not need to transmit it through any new channels—qualifying for and receiving paid family leave benefits from a federal program would require the exchange of significant personal and medical information, creating the opportunity for identity theft and wrongfully claimed benefits.

More Government Programs, More Avenues for Personally Identifiably Information Exposure. Governments and businesses are increasingly aware of the threats of identity theft, and most have taken measures to try to protect against identity theft.

The more government programs that individuals and families rely on, the more avenues exist for their personally identifiable information to be compromised.

While most governments work hard to protect their citizens' personal information, large programs create large room for error, and government agencies have been far from immune from data breaches. A few examples

Service, "The Child Tax Credit: How It Works and Who Receives It," updated November 17, 2020, https://fas.org/sgp/crs/misc/R41873.pdf (accessed August 1, 2021).

[31] Given the additional requirements that childcare providers would have to comply with to become a subsidized provider—things like childcare teachers needing college degrees, highly-prescribed rules dictating the precise infrastructure necessary to provide childcare, and government-mandated curriculums—the number of providers would be limited, with high-cost, urban areas likely offering the most choices and rural areas potentially having few or no subsidized providers available.

of large government data breaches over the past decade include:[32]

- 2011: The Texas Comptroller's Office revealed that 3.5 million Texans' personal information—including Social Security numbers—had been inadvertently placed on a publicly accessible state server for a full year.
- 2011: The security firm that oversees Tricare military health care, Science Applications International Corporation, experienced a data breach that included the personal information of 4.9 million military hospital and clinic patients.
- 2012: The South Carolina Revenue Department experienced a data breach in which 3.6 million Social Security numbers and 16,000 unencrypted credit card numbers were exposed.
- 2015: The U.S. Office of Personnel Management experienced two separate, but linked, intrusions that resulted in the breach of personal information on about 22 million federal employees, contractors, and others.

Moreover, while private businesses' viability depends upon them maintaining the privacy of their clients and individuals are free to choose which companies they provide their information, governments cannot go out of business for failing to protect their citizens' personal information, and individuals typically do not have a choice in providing their personal information to government agencies.

A More Effective, Lower-Risk Solution to Boost Individuals' and Families' Financial Security

The pandemic revealed that many Americans lack the savings they need to weather unexpected life events and loss of income. And even prior to the pandemic, it was already hard for families with young children to save for expected life events and costs such as taking family leave and paying for childcare.

Instead of establishing new government programs that leave less income in workers' and families' paychecks—or that effectively require kids to pay their own expenses by financing childcare subsidies and monthly child payments through increased debt—policymakers should let Americans keep more of the money they earn and make it easier for them to save it.

While many Americans can choose to save for college, for retirement, or for health care costs in specialized accounts, with rigid rules and restrictions, it is harder and more costly[33] to save for things like losing a job, having a car breaking down, needing to take family or medical leave, or paying for childcare.

Policymakers should establish universal savings accounts (USAs) so that all Americans can save and invest in a single, simple, and flexible account for any purpose, with no minimum contribution required, and without having to pay penalties or additional taxes upon withdrawal.[34] While not having enough money to save is a clear barrier to savings, a potentially equal or larger barrier can be the fear of not being able to access savings or having to pay early withdrawal penalties if workers and families need their savings for an unexpected expense.

USAs have been particularly helpful to lower-income and moderate-income households in

[32]Nate Lord, "Top 10 Biggest Government Data Breaches of All Time in the U.S.," Digital Guardian, October 6, 2020, https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time (accessed August 1, 2021).

[33]The reason non-specialized savings are more costly is that those savings are taxed twice; both as income when earned, and then again as capital gains, interest, or dividends before they are spent.

[34]Adam N. Michel, "Universal Savings Accounts Can Help All Americans Build Savings," Heritage Foundation *Backgrounder* No. 3370, December 4, 2018, https://www.heritage.org/taxes/report/universal-savings-accounts-can-help-all-americans-build-savings.

Canada and the United Kingdom, for instance, where low- and moderate-income individuals represent over 50 percent of account holders, and low- and moderate-income individuals save the highest percentages of their incomes.[35]

Moreover, instead of taking home smaller paychecks and then having to file for and submit personal identifiable information to many different government programs, the alternative of letting workers keep more of their earnings and allowing them to save in a single flexible account that they can use to directly purchase the things they want and need (without mandated release of their personal identifiable information), fewer Americans would have their personal information compromised.

Summary

Expanded unemployment insurance benefits were a necessary component of the federal government's economic response to the COVID-19 pandemic, but these programs' systematic failures, widespread fraud, and unintended economic effects should caution policymakers against making any of these unemployment insurance expansions permanent.

Even prior to these pandemic programs, large federal programs have been inherently plagued by excessive fraud and improper payment rates, sometimes exceeding 25 percent. And multiple government agencies have been subject to massive data breaches compromising tens of millions of individuals' personal information.

Criminals' exploitation of generous government programs to steal Americans' identities and taxpayers' dollars serves as a warning sign against the creation of new government programs that would simultaneously up the ante for criminals and establish new avenues for breaches of personally identifiable information. Instead of requiring individuals to pay higher taxes and submit their personal information to multiple government programs to obtain the things they need to support themselves and their families, policymakers should let Americans keep and save more of their own money so that they can use it on the things they want and need without being limited to what government programs will provide and without putting their personal identifiable information at risk.

[35]Organization for Economic Co-operation and Development, "Encouraging Savings Through Tax-Preferred Accounts," OECD *Tax Policy Study* No. 15, 2007, https://www.oecd-ilibrary.org/taxation/encouraging-savings-through-tax-preferred-accounts_9789264031364-en (accessed July 24, 2020).

****

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2020, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2020 operating income came from the following sources:

Individuals 66%
Foundations 18%
Corporations 2%
Program revenue and other income 14%

The top five corporate givers provided The Heritage Foundation with **1% of its 2020 income**. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position of The Heritage Foundation or its board of trustees.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM LIZ COYLE

Q.1. What are the risks of wire transfer fraud schemes connected to real estate closings?

A.1. New payment system technologies enabling faster payments directly from the payer to the payee offer potential benefits to consumers, but also may increase the risk of fraud or simply very costly mistakes. These increased risks are exposing consumers to fraudulent schemes tied to real estate closing transactions. Scammers hack into lenders' computers to access email addresses tied to pending transactions and send fraudulent emails tricking home buyers into wiring funds to the scammers' accounts rather than the intended financial institution. According to the National Credit Union Administration (NCUA), wire transfer scams involving real estate closings are increasing, based on a 2016 report of the Federal Bureau of Investigations.

Q.2. What can financial institutions do to alert their customers to suspicious transactions?

A.2. Federal and State regulators, financial institutions, payment system developers and other impacted or interested stakeholders should prioritize the development and implementation of cybersecurity, notification, fraud detection and prevention, and consumer awareness systems and regulations. Financial institutions should install stronger fraud and error resolution protections for their customers, including requiring the use of two-factor authentication. In 2021, the Federal Financial Institutions Examination Council (FFIEC) issued guidance titled Authentication and Access to Financial Institution Services and Systems "to provide financial institutions with examples of effective risk management principles and practices for access and authentication."

Q.3. How can financial institutions help people get their stolen funds returned?

A.3. Financial institutions should prioritize prevention to mitigate risk. Institutions should be held responsible for returning fraudulently stolen funds to customers. The Cyber Crime Support Network is an excellent resource for the industry, regulators, and victims of cybercrime.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM JOHN BREYAULT

Q.1. What are the risks of wire transfer fraud schemes connected to real estate closings?

A.1. Wire transfer fraud during real estate closings is a real risk to consumers that can be financially and emotionally ruinous. According to the Internet Crime Complaint Center, there were 13,638 victims of wire fraud in the real estate/rental sector in 2020 (a 17 percent increase over 2019), with losses of more than $213 million.[1] According to a recent survey by the American Land Title As-

[1] Federal Bureau of Investigation Internet Crime Complaint Center. "Internet Crime Report 2020". March 17, 2021. Online: *https://www.ic3.gov/Media/PDF/AnnualReport/2020-IC3Report.pdf.*

sociation, cybercriminals attempted to trick employees into wiring funds to a fraudulent account in a third of all real estate and mortgage transactions. Full recovery of lost funds was only possible in 29 percent of cases involving wire fraud targeting title agencies. In 40 percent of the cases, less than 10 percent of the funds were recovered. [2]

Wire fraud targeting real estate closings affects participants in all phases of the closing, including title companies, law firms, real estate agents, buyers, and sellers. A typical scenario begins with a hacker gaining access to a title company's or lender's email server and searching for upcoming real estate closings. [3] Fraudsters may also search Multiple Listing Service websites such as Trulia or Zillow to identify pending home sales and the associated parties in those transactions. [4] The fraudsters then send spoofed emails to participants in one or more closings. The emails may appear to come from a transaction participant and typically contains instructions directing the recipients to change the payment type and payment location so that payments go to accounts controlled by the fraudsters. If the funds are sent to a fraudulent account, they are typically quickly obtained by the scammers via cash or check withdrawals. Because the disbursement of funds from the fraudulent accounts tend to occur so quickly, it is often difficult or impossible for the payment to be canceled or for lost funds to be recovered when the fraud is discovered. [5]

Q.2. What can financial institutions do to alert their customers to suspicious transactions?

A.2. Consumer education at the beginning and repeated warnings throughout the closing process can help increase consumer awareness of this scam. For example, financial institutions should provide alerts to borrowers to educate them about the warning signs of real estate wire fraud at multiple points during the home-buying process. Financial institutions should also work with borrowers, title agents and other participants in the real estate closing process to verify that wire transfers are not being sent to fraudulent accounts. Resources such as the American Land Title Association's "Outgoing Wire Preparation Checklist" and "Rapid Response Plan for Wire Fraud Incidents" are valuable resources for helping participants in real estate transactions reduce their risk of wire fraud. [6]

Q.3. How can financial institutions help people get their stolen funds returned?

A.3. Financial institutions should make consumer education about what do when wire fraud is suspected a regular part of their inter-

---

[2] American Land Title Association. "Survey: Title Professionals Targeted for Wire Fraud in a Third of all Transactions". April 20, 2021. Online: *https://blog.alta.org/2021/04/survey-title-professionals-targeted-for-wire-fraud-in-a-third-of-all-transactions.html.*

[3] National Credit Union Administration. "Wire Transfer Scams Involving Real Estate Transactions Are Increasing". 2018. Online: *https://www.ncua.gov/newsroom/ncua-report/2018/wire-transfer-scams-involving-real-estate-transactions-are-increasing.*

[4] Bay National Title Company. "Real Estate Wire Fraud: How To Stay Protected When Buying a Home". Online: *https://www.bntc.com/wire-fraud/.*

[5] Federal Bureau of Investigation. "Public Service Announcement: Business E-mail Compromise the 12 Billion Dollar Scam". July 12, 2018. Online: *https://www.ic3.gov/Media/Y2018/PSA180712.*

[6] American Land Title Association. "Protect Your Money". Online: *https://www.alta.org/business-tools/wirefraud.cfm.*

actions with borrowers. Acting quickly when wire fraud occurs is a key factor in increasing the chances that funds sent via fraudulent wire transfers can be recovered. Congress should also consider legislation that would redefine the Federal Reserve's definition of "unauthorized transactions" to cover incidents where consumers are induced to send money for fraudulent purposes.

Q.4. How can financial institutions monitor accounts for suspicious activities?

A.4. Financial institutions should ensure that their fraud detection systems are as up to date as possible. While no system is foolproof when it comes to detecting and preventing wire fraud, financial institutions must make it a priority to invest in antifraud controls that reduce the risk of wire fraud.

Q.5. Financial institutions know that multiple transactions under $10,000 may be suspicious; should multiple transactions of smaller amounts also be flagged for fraud if they seem suspicious?

A.5. Yes. Multiple multithousand-dollar transactions over a short period of time, particularly if the source is an account that does not typically engage in such transactions, should be a signal of potential fraud. While transactions smaller than $10,000 may not be indicative of wire fraud associated with real estate closing, fraudsters are known to request payment via wire transfer for many other types of fraud. Such transactions may also indicate that the sending account in engaged in activity consistent with "money mules" or other accomplices (witting or otherwise) in fraud.

Q.6. What are the responsibilities for financial institutions to question their customers on suspicious withdrawals?

A.6. Financial institutions often train their frontline employees to question customers when the customer makes suspicious withdrawals. However, fraudsters are known to quickly adapt to such tactics, even coaching victims on what to say in response to questioning by financial institution employees. We would also encourage financial institutions to consider whether certain customers are at high risk of engaging (knowingly or not) in fraudulent transactions and develop systems to appropriately challenge suspicious transactions by those who are at high risk.

Q.7. Are there transactions where a second person, like a spouse or adult child, should be contacted to verify withdrawals?

A.7. For customers who are at high risk of being victims of fraud, we believe it is appropriate for financial institutions to contact trusted parties such as spouses or adult children to verify withdrawals before such withdrawals are processed.

Q.8. Do financial institutions flag overseas withdrawals for accounts that do not typically have them, especially for people over 65 years of age?

A.8. I am not aware of specific financial institutions that do this or regulations that would require financial institutions to flag such withdrawals. However, I believe that this is an area that would be ripe for further investigation by the Committee and regulatory agencies.

Q.9. What kind of holds should financial institutions have for overseas transactions that seem unusual?

A.9. A key benefit for fraudsters engaged in wire fraud is that received funds can often be obtained quickly, with little recourse for the sending party if fraud is discovered or suspected after the fact. For high-risk accounts, we believe that controls should be put in place that would place holds on overseas transactions that have indices of potential fraud. This would give customers and sending institutions additional time to investigate and verify suspicious transactions before fraudsters are able to obtain the funds.

Q.10. How can financial institutions flag fraud where the scammer has misled the victim and the victim thinks the transactions are legitimate?

A.10. Financial institutions should be willing to place holds on transactions that have indices of fraud, even if the customer thinks that the transaction is legitimate. However, we believe that a comprehensive solution should also include new protections that would place more liability on financial institutions when account holders are induced to authorize sending money to fraudsters. Such liability shifting would not only make it more likely that defrauded consumers can be made whole, it would also create a powerful incentive for financial institutions to invest in systems that would reduce the risk of fraud occurring in the first place.

Q.11. What legal assistance is available for victims of fraud? How do victims know they can—and should—file complaints with local governments, legal aid, the Federal Trade Commission, the Consumer Financial Protection Bureau, etc.?

A.11. It is too often incumbent on fraud victims themselves to seek out legal assistance. Fortunately, agencies like local police departments, State Attorneys General, legal aid service providers, and Federal resources from the Federal Trade Commission and the Consumer Financial Protection Bureau do a relatively good job at making their services findable online. However, given the significant number of consumers who either lack access to the Internet or who are uncomfortable with or unable to use technology, there is always the need for providers of legal assistance for fraud victims to proactively reach out to victims and potential victims of fraud.