OVERSIGHT OF THE FINANCIAL CRIMES ENFORCEMENT NETWORK

HYBRID HEARING

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

APRIL 28, 2022

Printed for the use of the Committee on Financial Services

Serial No. 117–81

U.S. GOVERNMENT PUBLISHING OFFICE
47–648 PDF WASHINGTON : 2022

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
ALMA ADAMS, North Carolina
RASHIDA TLAIB, Michigan
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
NIKEMA WILLIAMS, Georgia
JAKE AUCHINCLOSS, Massachusetts

PATRICK MCHENRY, North Carolina, *Ranking Member*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas
PETE SESSIONS, Texas

CHARLA OUERTATANI, *Staff Director*

CONTENTS

WITNESSES

THURSDAY, APRIL 28, 2022

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

OVERSIGHT OF THE FINANCIAL CRIMES ENFORCEMENT NETWORK

Thursday, April 28, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The committee met, pursuant to notice, at 10:05 a.m., in room 2128, Rayburn House Office Building, Hon. James A. Himes presiding.

Members present: Representatives Velazquez, Sherman, Meeks, Green, Cleaver, Perlmutter, Himes, Foster, Beatty, Vargas, Gottheimer, Gonzalez of Texas, Axne, Casten, Lynch, Adams, Tlaib, Dean, Garcia of Illinois, Williams of Georgia, Auchincloss; McHenry, Posey, Luetkemeyer, Huizenga, Wagner, Barr, Williams of Texas, Hill, Emmer, Zeldin, Loudermilk, Mooney, Davidson, Budd, Kustoff, Hollingsworth, Gonzalez of Ohio, Rose, Steil, and Timmons.

Mr. HIMES. [presiding]. The Financial Services Committee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time.

Today's hearing is entitled, "Oversight of the Financial Crimes Enforcement Network."

I now recognize myself for 5 minutes to give an opening statement.

Today, we welcome Mr. Himamauli Das, the Acting Director of the Financial Crimes Enforcement Network, also known as FinCEN, for the first time before our committee. At a time when the international community is united in imposing severe sanctions on Russia for its unprovoked attack on Ukrainian sovereignty and democracy, a strong, well-resourced FinCEN is more important than ever.

FinCEN is on the front lines of our financial intelligence efforts, tracking and tracing the ways that bad actors, like Putin and his allies, try to hide their assets. FinCEN also provides law enforcement agencies with information to follow the money, and alerts financial institutions to the ways that bad actors might try to evade sanctions. Without FinCEN, terrorists, drug traffickers, and other criminals would pose an even greater threat to our national security and the integrity of our financial sector.

Lately, this committee has focused hard on cracking down on oligarchs and other bad actors looking to hide their ill-gotten gains through financial channels. Last month, the committee passed several bills to further cut Russia off from the global markets, to iso-

late Russian officials on the international stage, and to target Russian oligarchs, including the Nowhere to Hide Oligarchs' Assets Act, which was led by Chairwoman Waters. Today, I am pleased that we will continue discussing these bills and other proposals to target financial crime schemes, including a bill that I have sponsored, the Special Measures to Fight Modern Threats Act, which would help FinCEN target money laundering concerns operating outside of the traditional banking sector.

In the past, this committee, and Chairwoman Waters in particular, played an important role in passing the Anti-Money Laundering Act of 2020 (AMLA), which was the most sweeping anti-money laundering reform in decades. AMLA tasks FinCEN with zeroing in on corruption, cybercrime, foreign and domestic terrorist financing fraud, transnational criminal organization activity, and trafficking. It also contains the Corporate Transparency Act, which requires corporations to disclose their true beneficial owners and tasks FinCEN with implementing this transformative anti-corruption measure. In the 15 months since AMLA became law, FinCEN has made considerable progress on these tasks, despite delays in authorized funding. But there is more work ahead to do, and more regulations to be finalized to ensure that law enforcement can use these important tools to follow the money and bring bad actors to justice.

Even before Russia's illegal invasion of Ukraine, FinCEN helped protect our financial sector from money launderers, authoritarians, and kleptocrats. Today, as some of the richest and most corrupt people in the world look to the United States to stash their dirty money, it is important that Congress and this committee give FinCEN the resources it needs to assure that Putin, his cronies, and his despots and thugs don't get access to our financial system to hide their money.

It is also important that FinCEN be transparent with Congress about its accomplishments, its challenges, its strengths and its weaknesses, and to share findings that can help lawmakers who are tasked with oversight to better understand FinCEN's strengths and weaknesses. FinCEN and Congress must work together to make sure that our financial crime toolkit is being put to good use, and that we are staying vigilant against emerging threats and sanction evasion schemes.

Finally, I would like to enter into the record statements from the Project on Government Oversight, The Sentry, and the FACT Coalition. These statements emphasize FinCEN's critical role in combating corruption, and stress the importance of a fully-funded and staffed FinCEN to implement the beneficial ownership reporting requirements as envisioned by Congress.

Without objection, it is so ordered.

Mr. Das, I look forward to your testimony on the implementation of the Anti-Money Laundering Act of 2020, and FinCEN's progress on the beneficial ownership database, and to learning more about how Congress can be a strong and reliable partner in helping FinCEN successfully combat financial crime.

I now recognize the ranking member of the committee, the gentleman from North Carolina, Mr. McHenry, for 5 minutes.

Mr. MCHENRY. Thank you, Mr. Himes, and thank you for sitting in the chair. We wish Chairwoman Waters a speedy recovery from COVID, and we are glad that she is getting the care she needs and taking the responsibility of separating and quarantining. We wish her a speedy recovery.

But I want to thank the Chair for holding the hearing. As we know, the proper oversight of agency heads is necessary for Congress' intent to be fulfilled and for agencies to fulfill their responsibilities. For an office like FinCEN, which has operated under the radar screen for the last 3½ years, appearing before us is especially significant. Acting Director Das, thank you for being here. Thank you for your outreach.

Mr. Das, you were not head of FinCEN during the Fiscal Year 2021 National Defense Authorization Act (NDAA) negotiations, which resulted in a rewrite of the statute that you are now implementing. But I would like to take a moment to share with you congressional intent during those negotiations, and the resulting statute and the intent of that statute. And the reason why I want to do this is because in reading FinCEN's beneficial ownership notice of proposed rulemaking (NPRM), there seems to be quite a disconnect.

Early negotiations were anything but bipartisan. For Republicans, non-negotiables were clear. We wanted to limit burdens on small businesses, protect personally identifiable information (PII) as if it were tax information, and hold FinCEN accountable to the American people once a bill became law. We understood on both sides of the aisle that the stakes were too high for millions of small businesses to not get this right. So, the four corners in our negotiations came to an agreement that a revised beneficial ownership regime would: first, be easy to understand for small businesses; second, limit the burdens on those filing; and third, protect civil liberties and ensure confidentiality.

What resulted was a targeted statute that would focus on stopping bad actors, such as Chinese and Russian nationals, from using the financial system. At the same time, it limited the burdens of law-abiding small businesses in the process. We directed FinCEN to prevent duplicative and burdensome requirements on small businesses, including rescinding the customer due diligence rule. We directed FinCEN to report on steps it is taking to minimize reporting requirements, which will provide this committee with necessary data on suspicious activity reports (SARs), currency transaction reports (CTRs), and the reporting thresholds. And we asked that the new beneficial ownership data be equipped with the strongest privacy and disclosure protections for small business owners' information.

FinCEN is one of the biggest data collectors in the U.S. Government. Yet, how they collect, manage, and allow access to that data remains largely a mystery to Congress and, most assuredly, the public. Unfortunately, after reading FinCEN's NPRM, it is clear that the Agency needs a reminder of what Congress directed. The proposed rule was far too complex, overly broad, and deviated significantly from Congress' intent. My colleagues across the aisle like to advocate for greater authorities for FinCEN. I understand that. We have a new statute. The rules have not been implemented on

that new statute. Let's get that done before we talk about new authorities, and I think that is where we are at this stage.

And without objection, I would like to submit for the record my letter with Ranking Member Luetkemeyer, outlining our disappointment and concerns with the beneficial ownership NPRM. Thank you.

Mr. HIMES. Without objection, it is so ordered.

Mr. MCHENRY. Director Das, it is fair to say that FinCEN has too many responsibilities and doesn't do any of them as well as they could. I am hopeful that in your leadership of FinCEN, we can right some of these huge challenges for the Agency and get it right for the American people. And I look forward to working with you to ensure that our anti-money laundering programs are targeted and effective, and at the same time, protect Americans' civil liberties.

With that, Mr. Chairman, thank you, and I yield back.

Mr. HIMES. Thank you to the ranking member. I now recognize the gentleman from Kentucky, Mr. Barr, for 1 minute for an opening statement.

Mr. BARR. I thank the Chair for yielding and for holding this hearing today.

Congressional oversight of FinCEN is long overdue. Acting Director Das, thank you for coming before us today to talk about the operations of FinCEN. FinCEN indeed has a critical mission, and safeguarding the financial system against illicit use has never been more important. Whether FinCEN is targeting Russian oligarchs, international terrorists, or narcotics traffickers, we need to hold your office accountable for results. At times, this will mean FinCEN investigators need to find a needle in a haystack. Congress supports this work, but FinCEN must also guard against the temptation to add to the haystack endlessly, simply so it can collect more and more data on Americans. FinCEN's intelligence should be used as a weapon against money launderers, not as a financial Wikipedia on law-abiding citizens. I look forward to hearing how FinCEN can stay focused on its targeted mission, including its efforts to counter bad actors from Russia.

Thank you for your testimony, and I yield back.

Mr. HIMES. The gentleman yields back. I want to welcome today's distinguished witness to the committee, Mr. Himamauli Das, the Acting Director of the Financial Crimes Enforcement Network.

You will have 5 minutes to summarize your testimony, Mr. Das. You should be able to see a timer that will indicate how much time you have left. I would ask you to be mindful of the timer and quickly wrap up your testimony if you hear the chime.

And without objection, your written statement will be made a part of the record.

Acting Director Das, you are now recognized for 5 minutes.

STATEMENT OF HIMAMAULI DAS, ACTING DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

Mr. DAS. Good morning. My name is Him Das, and I am the Acting Director of the Financial Crimes Enforcement Network. Chairman Himes, Ranking Member McHenry, and distinguished members of the committee, thank you for the invitation to appear before

you today to provide an update on FinCEN's implementation of the Anti-Money Laundering Act of 2020, including the Corporate Transparency Act.

FinCEN fulfills a critical statutory mandate as the administrator of the Bank Secrecy Act (BSA). In that role, we draft regulations to implement the BSA, we receive statutorily-required reports from financial institutions about things like suspicious activities and high-value cash transactions, and we regulate financial institutions and enforce the rules. We can and have imposed significant monetary penalties against financial institutions that failed to implement effective and reasonably-designed Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) programs. Our statutory authorities give us a powerful toolkit that we use to protect the U.S. national security and safeguard the integrity of our financial system. Along with suspicious activity and cash transaction reports, we can request information from financial institutions, and in some cases, non-financial trades and businesses within defined parameters through special collection tools.

We use the information that financial institutions report to us to support law enforcement to target and disrupt illicit finance threats. And it is a diverse set of threats, from cyber criminals to kleptocrats, organized crime groups and beyond. Our information and analysis is critical to combat all of them. In fact, in a survey released in 2020, the Government Accountability Office found that law enforcement personnel at six law enforcement agencies use BSA reports extensively to inform their investigations, and that BSA reporting helped to identify potential subjects, networks, and defendants.

Recent events, from COVID-19 to Russia's invasion of Ukraine and the rise in ransomware attacks on U.S. businesses, have underscored the importance of protecting our financial system. They have made clear the importance of an AML/CFT framework that is well-designed and effective in preventing bad actors from exploiting the financial system, and that protects Americans and American ideals. Clearly, FinCEN has a robust agenda and a diverse mission. And while we work to carry out our statutory mandate, we are also cognizant of our responsibility to do so in a way that safeguards citizens' privacy, that does not put undue burden on small businesses, and that does not spark de-risking that harms financial inclusion. All of these considerations are important to me and to our institution.

The AML Act has only expanded our responsibilities, and it is nothing short of transformative. We recognize the enormous opportunity that it presents to streamline, modernize, and update the U.S. AML/CFT regime. The Act has helped position us to address today's challenges and provides us with the tools to approach innovations in a way that balances opportunities and risks, and it has placed national security front and center in FinCEN's mandate.

While the AML Act has made a significant improvement to the AML/CFT framework, these improvements come at a cost. FinCEN employs a team of about 300 dedicated employees: intelligence analysts; investigators and enforcement officers; policy strategists; data analysts; and others. We welcomed the Fiscal Year 2022 appropriations to support our mission. Those resources are critical to support

our IT systems and to build our beneficial ownership database. But nonetheless, FinCEN has significant staffing requests that remain unfunded. These include requests specifically related to positions required in the AML Act, such as foreign Financial Intelligence Unit (FIU) liaisons, domestic liaisons, and others.

Timely and effective implementation of the AML Act is our top priority. Even with our limited resources, the FinCEN team is working diligently with law enforcement and regulatory stakeholders to promulgate rules and take other steps under the Act to promote a transparent financial system. It is important that we get it done right, and we get it done quickly. We have accomplished a lot, but we also recognize that we need to do more. As you are aware, we are missing deadlines. And to be blunt, we will likely continue to do so because our budget situation has required us to make significant tradeoffs among competing priorities.

Just as I am grateful for the opportunity to appear before you today, I am also glad that I have had the opportunity to speak with some of you in the lead-up to today's session to hear more about your priorities and what is most important to your constituents. The entire FinCEN team is committed to working with you and to carrying out our ambitious agenda with your support, and I am happy to answer any questions.

[The prepared statement of Acting Director Das can be found on page 50 of the appendix.]

Mr. HIMES. Thank you, Acting Director Das. I now recognize myself for 5 minutes of questions.

Mr. Das, I read your testimony and just listened, and I appreciate all of that testimony. What I would love to have you do first in my 5 minutes is maybe fill in some of the blanks, which are really critical oversight blanks from what we have heard so far, that is, how FinCEN defines success. I would assume it would be prosecutions assisted in, nefarious plots disrupted. How do you quantify and, therefore, know when you are succeeding and where you may succeed better? I am used to thinking in the intelligence context, where the intelligence community looks at the number of citations for collection and in various reports and that sort of thing.

And then second, if we have time, the other thing we obviously need to do is protect the privacy of the American people, and I am very grateful for the data that you have provided my office with respect to the collection that you do. How do you evaluate and how do you raise incidents of privacy breaches that, from an oversight standpoint, we should be interested in? But, again, I am primarily interested in how you define success and what metrics allow you, and therefore us, to track that success.

Mr. DAS. Thank you for that question, Chairman Himes, and thank you for your support and the committee support as well. Again, we are very focused on measuring and ensuring success in achieving FinCEN's mission. We think it is incredibly important to engage with stakeholders in Congress on ensuring the effectiveness of BSA reporting, and it is absolutely critical to ensuring confidence in the AML/CFT framework.

Again, I just want to step back for a second. FinCEN has a number of functions, right? We collect information and reports from financial institutions, we issue regulations that regulate financial in-

stitutions to ensure that they have successful and effective and reasonably designed AML/CFT programs as well, and we work closely with law enforcement, and the intelligence community, and the Office of Foreign Assets Control (OFAC) in ensuring that they receive and use our information in an effective way. We want to be effective on all of these fronts because all three components of our mission work together.

In terms of your specific question on the success of reporting, the AML Act provides a framework for that. Section 6201 of the AML Act does precisely that. It requires DOJ to provide a report on the value of BSA information, and in January of this year, DOJ delivered such a report. That reports states that the value of BSA information for DOJ cannot be overstated. IT staff has searched BSA records over 2 million times over the past 5 years, and it is used in tens of thousands of investigations. The GAO, in a survey conducted from the years 2015 to 2018, as well indicated that three-fourths of the staff of six law enforcement agencies have used BSA reporting in the context of their investigations. And that study also noted that three-fourths of those personnel also indicated that they either did not have an alternative, or that an alternative to BSA reporting was less efficient. I recognize, however, that the information that I have provided is our qualitative measures of success. They are not quantitative measures of success.

Mr. HIMES. Mr. Das, that is interesting information about the DOJ. I think you told me that there are just shy of 500 law enforcement agencies that have access to the database. When they query that database, are they then required to report what they did with the information that was obtained as part of that query, therefore enabling you to see what the outcome is of the use of that information?

Mr. DAS. They are not required to respond specifically to the use of the data that they receive when they do a query. However, we proactively engage with law enforcement across-the-board. We have a number of liaison officers from law enforcement agencies who sit at FinCEN, whom we engage with regularly in terms of the challenges that they are facing, in terms of using our data, how they use their data, and how we can help them more effectively use their data. We regularly engage with our law enforcement counterparts and provide products to them. We flag—

Mr. HIMES. I'm sorry. Thank you. In my last 20 seconds, the data is important, but so are the anecdotes. We are very focused on Ukraine and Russia right now. In my very limited remaining time, tell us what FinCEN is doing, maybe an anecdote or a story, an example of how you have used this data to go after oligarchs or otherwise illicitly—

Mr. DAS. Absolutely. We have identified over 2,000 suspicious activity reports (SARs) that relate to Russian oligarch activity and Russian sanctions evasion. We have reviewed all of those reports. We have sent 271 of those reports to law enforcement, and to OFAC, and the intelligence community to understand what is happening with respect to illicit financial transactions, which they can use for prosecutions, and to trace assets and seize and freeze assets. The information that we receive, we have also provided directly to OFAC, so that they can use it in their sanctions investiga-

tions and then designate and target illicit actors across-the-board, including Russian oligarchs, shell companies, cryptocurrency companies, and others. A number of the recent actions were based on information that we have provided to OFAC as well.

Mr. HIMES. Thank you, Mr. Das. My time has expired.

The ranking member of the committee, Mr. McHenry, is now recognized for 5 minutes.

Mr. MCHENRY. Thank you, Mr. Chairman. And thank you, Acting Director Das.

I think there is a lot of confusion about what FinCEN does. And I want to piggyback on Mr. Himes' question here, but let's just kind of walk through the basics. Last month, there were roughly 325,000 suspicious activity reports filed with FinCEN. That is a massive amount of data. Let's talk through what FinCEN does with this sort of flood of data. What percentage of Bank Secrecy Act reports and FinCEN's monthly database lead to convictions?

Mr. DAS. I appreciate the question, Ranking Member McHenry. Again, we do not have precise metrics in terms of a one-to-one correlation between information that we receive from financial institutions with respect to suspicious activity reports and direct prosecutions. But in response to the DOJ report, it is clear that these reports are being used by the Justice Department and by other law enforcement agencies to investigate actions and to prosecute actions as well. We have had a law enforcement awards program in place since 2015, and that law enforcement awards program is designed to identify instances in which BSA information has translated into actual prosecutions. So it is anecdotal in nature, but it shows that our information is being used by law enforcement, especially the—

Mr. MCHENRY. The anecdotes here are very few and far between. We have talked about this, so I think that is a problem. Mr. Himes' question and my follow-up to basically the same question here is, show us the results. You are able to talk about what you said as qualitative rather than quantitative. We would like to see these statistics on what is being done. Mr. Himes said that 500 individual agencies have access to these databases, the currency transaction reports, and suspicious activity reports, 500 agencies. How many individuals have access to these databases?

Mr. DAS. Thank you for that question. Your first point, in terms of metrics and better understanding how the information is being used, we intend to work with you as well as the law enforcement agencies to hone those metrics and to provide better assessments of how that information is being used. In terms of the number of individuals who have access to the database, from law enforcement, from the intelligence community and other agencies as well, again, there are 471 agencies that have access to the information. The number of law enforcement personnel and other personnel who have access fluctuates, but it is in the 13,000 to 16,000 range.

Mr. MCHENRY. Okay. Then, how do you keep track of how those users use that information? How do you police that?

Mr. DAS. I appreciate the question. We have a robust framework in place. With respect to each of the 471 agencies, we negotiate separate memorandums of understanding (MOUs) with each of the agencies after having a discussion with them to ensure that they

have appropriate reasons under the purposes of the Bank Secrecy Act to use that information. The MOUs identified protocols for access, protocols for security, and protocols for use of that information.

Mr. MCHENRY. But how do you police those MOUs?

Mr. DAS. It is part of sort of an overall suite of efforts in terms of those MOUs. In terms of access to the database, individuals who have access need to go through a robust training program. They need to undergo a background check. Each of their searches—

Mr. MCHENRY. Okay. So, what is then the proscriptive?

Mr. DAS. We track each of their searches. They need to enter in a justification. It goes into a query audit log, and then we do two things. One is we conduct an annual audit of the searches that are being done by each of the agencies that have access to ensure that they are being used appropriately and that there is no misuse. We engage with the agencies on an individual basis to ensure that there are no questions and that all questions are answered. And then finally, we identify anomalous searches on a quarterly, on a monthly, and on an annual basis to identify whether or not there are any inappropriate uses of the database, and we reach out to the agencies to try to remedy that as well.

Mr. MCHENRY. Okay. I want to be respectful of everyone's time, but what if an MOU is breached, or if individuals have breached that responsibility, what is the enforcement action?

Mr. DAS. We will do two things. First of all, we will engage with the agency and seek responses to an investigation in terms of what that individual is doing, and whether or not they were doing it appropriately, and we will refer the issue to the Inspector General's office as well.

Mr. MCHENRY. Okay. Would you provide data on that, on those referrals?

Mr. DAS. Yes, sir. We can.

Mr. MCHENRY. Thank you. Thanks for your testimony.

Mr. HIMES. The gentleman's time has expired.

The gentlewoman from New York, Ms. Velazquez, who is also the Chair of the House Committee on Small Business, is now recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. Director Das, in December of 2019, FinCEN released a statement entitled, "Bank Secrecy Act Reports Filed by Financial Institutions Protect Elders from Fraud and Theft of Their Assets." In this statement, former FinCEN Director, Ken Blanco, acknowledged that understanding the trends and potential exploitation methods included in these reports can help banks and consumers protect themselves. Can you briefly tell us how financial institutions and older consumers use these reports to protect themselves from financial exploitation?

Mr. DAS. Thank you, Congresswoman Velazquez. Elder abuse is a terrible problem and one that we and our partners from across the government have been focused on for many years, and we provide ongoing support to numerous task forces and multi-agency groups working to address this problem. In February, we joined with other Federal agencies in an awareness-raising campaign about romance scams, which often target the elderly. In this campaign, we highlighted our Rapid Response Program. In this pro-

gram, FinCEN partners with law enforcement agencies that receive complaints of abuse, and incorporates with Foreign Financial Intelligence Units, our counterpart agencies in foreign governments, to help recover stolen funds.

We have done a lot more on this front, too. Our first public advisory to financial institutions on elder financial exploitation dates back to 2011. Since then, in 2017, we issued a joint memorandum with the Consumer Financial Protection Bureau (CFPB) on financial institution and law enforcement efforts to combat elder financial exploitation. In 2019, we issued a financial trend analysis describing how our elders face increased financial threats from domestic and foreign actors, and it is critical that we work with law enforcement, regulatory, and national security partners to use our information. Public documents like the one I just mentioned that highlight typologies, educate financial institutions so that they can appropriately use risk-based mitigating measures, and monitor to detect potential elder abuse. This ultimately protects consumers. And this reports also led to an incredible increase in SAR reporting, and has ultimately led to numerous successful prosecutions of bad actors.

Ms. VELAZQUEZ. Thank you for the response. Director Das, like elders, survivors of intimate partner violence are at high risk of financial exploitation. In fact, 58 percent of survivors, approximately 19.1 million individuals in the United States, report that their abuser has accessed, withdrawn from, or otherwise controls their bank account. This means that over half of survivors in the U.S. do not have access to a safe and protected bank account. Wouldn't you agree this is a significant problem that must be addressed?

Mr. DAS. Thank you for that question. I agree that victims of domestic violence and all victims of financial abuse should be able to obtain banking access and extricate their accounts from their abuser. We are very focused on financial inclusion, and we want to work with you and your offices to ensure that FinCEN does its part to ensure that survivors have access to the banking services.

Ms. VELAZQUEZ. Thank you. One of the bills that we are reviewing here today is a discussion draft of legislation I am working on, the Survivors Safe Banking Act, which will require FinCEN to compile and publish reports on statistics and trends of customers and potential customers of covered financial institutions who are a survivor of domestic violence or economic abuse. Wouldn't you agree that a similar report will likewise help protect consumers who are survivors of intimate partner violence from financial exploitation?

Mr. DAS. Thank you, Congresswoman. Without commenting on the specifics of the draft legislation, FinCEN has and will continue to urge financial institutions to report all forms of suspicious transactions and to be attentive to any abnormal patterns or behaviors, whether in their customer's accounts or in their interactions with them. Again, as you are well aware, and as FinCEN has highlighted through advisories and notices and alerts, there are a myriad of illicit finance threats facing consumers today. And sadly, vulnerable populations, such as the elderly, or those in abusive relationships can be victimized and financially exploited by those close to them. We will continue to educate and equip financial institu-

tions on these threats, what to look for, and how to report a suspicious transaction.

Ms. VELAZQUEZ. I am looking forward to working with you.

Mr. DAS. Thank you. As am I.

Ms. VELAZQUEZ. Thank you. I yield back.

Mr. HIMES. The gentlelady's time has expired.

The gentleman from Florida, Mr. Posey, is now recognized for 5 minutes.

Mr. POSEY. Thank you very much, Mr. Chairman. Mr. Das, can you please describe your strategic plan for protecting the privacy of the individuals and firms you collect data from?

Mr. DAS. Pardon me, Congressman, if you could repeat your question? It didn't quite come through clearly. My apologies.

Mr. POSEY. Could you please describe your strategic plan for protecting the privacy of the individuals and firms you collect data from?

Mr. DAS. Yes. Thank you, Congressman. Again, that is a very important issue for us. The privacy of our database and the sensitive information that we collect is fundamental to me and is fundamental to our institution more generally. We have a number of processes in place to ensure that the information is safeguarded and used appropriately, and we are continuing to work to do more on this front, to identify any gaps or issues and to remedy those gaps. We have a robust framework in place both from an IT perspective and from a procedural perspective in ensuring and safeguarding the use of this information. From an IT perspective, we have robust controls and a significant segment IT architecture, which is robust, and constrains access to the database by hackers and other malicious threats to the database.

Second, we conduct regular penetration testing to ensure that the database is not exposed to malicious threats as well, and we subject the database to the highest standards of security controls. It is Federal Information Security Modernization Act (FISMA) high level with respect to the security structure of the IT database.

With respect to the privacy considerations, again, as I mentioned previously, we have robust controls in terms of access to the data and the use of the data. We negotiate MOUs in place with each of the agencies that have access to our database. Those MOUs include provisions which ensure that the database is used appropriately and that there are appropriate audit and oversight functions. We provide regular training to those who have access to the database to ensure that they understand what the parameters are in terms of their use of the database, and that they use it appropriately and for purposes that are consistent with their agency's access to the database, and consistent with the purposes of the Bank Secrecy Act as well.

And then, we audit those uses. Again, we have a query audit log where we track each of the searches and the justifications made for those searches. Where there are anomalous searches, we refer those searches and concerns to the home agency as well as to the Inspector General's Office. We investigate, and if there are shortcomings in terms of those searches, we work with the agencies to either restrict access or to terminate those individuals.

Mr. POSEY. Have there ever been any breaches?

Mr. DAS. There have been no IT breaches that we are aware of to the overall database.

Mr. POSEY. Does FinCEN share information and data with the Internal Revenue Service?

Mr. DAS. One of the purposes of the Bank Secrecy Act, in terms of use of the information, is to combat tax evasion, and the IRS has access to our database to support their law enforcement efforts and efforts to combat tax evasion. The IRS Criminal Investigations Unit as well is a partner in our—

Mr. POSEY. I think that is a yes.

Mr. DAS. Pardon me?

Mr. POSEY. I think that is a yes, isn't it?

Mr. DAS. It is a yes.

Mr. POSEY. Can you explain the cost-benefit analysis in your rulemaking and how that compares with other agencies?

Mr. DAS. Yes, sir. We conduct cost-benefit analyses under the Regulatory Impact Act for each of our rulemakings. It is required by law. And when we renew regulations, as we are required to do on a periodic basis, we conduct cost estimates in terms of what the cost might be with respect to those regulation renewals.

Mr. POSEY. Thank you very much. Mr. Chairman, my time is about to expire, so I yield back. Thank you.

Mr. HIMES. The gentleman yields back.

The gentleman from Missouri, Mr. Cleaver, who is also the Chair of our Subcommittee on Housing, Community Development, and Insurance, is now recognized for 5 minutes.

Mr. CLEAVER. Thank you very much. I have a number of questions that I would like to raise with you, Acting Director Das. Compared to many, probably most of the Federal agencies, you are a small, either an agency or a bureau; I am not sure which is the appropriate term. But I am wondering, Congress approved $161 million and the President had requested $191 million. Does the fact that we didn't meet the President's request have any negative impact on your work?

Mr. DAS. Thank you for that question, Congressman. We are a bureau of the Treasury Department. We have 300 full-time equivalents (FTEs) at this point. First of all, I want to express my appreciation for the funding in the Fiscal Year 2022 appropriations. We received about $34 million over previously-enacted levels in that legislation. And that funding is incredibly important to us in terms of being able to ensure operations of our IT system and our IT database. It is also incredibly important in terms of our design and build of the beneficial ownership database. So, it is a valuable contribution in terms of our overall effort.

It does fall short, however, in terms of our ask of, I believe, $64.5 million over previously-enacted levels. The amount of money that we did not get was intended to be used for FTE staffing for all of our efforts to implement the AML Act. We had asked for 80 FTEs to support our staffing and implementation of the AML Act. That includes drafting regulations and the rules being able to conduct the cost-benefit analyses and to perform all of the other functions under the AML Act, including hiring foreign FIU liaisons, and domestic liaisons to do outreach to financial institutions across the country to help them understand how we use data and how it is

effective. It would be used to hire innovation officers, and security and information officers as well, who would be able to help steer and lead the charge with respect to our engagement on innovative technologies and how the regulatory framework meets the innovative technologies as well. Again, even with the resources that we have and that we are using, we are working full tilt to be able to work thoroughly, and effectively and efficiently, to complete all of the mandates required under the AML Act, but we need more.

Mr. CLEAVER. Yes, you just hit on the point that I was going to raise, which is what is not getting done because you didn't receive the amount that was requested in the President's budget. And I am assuming you are saying that everything is getting done; it is just not at the level that the Bureau required.

Mr. DAS. I have two points on that. One is that we are missing deadlines, as I mentioned in my testimony, and we will continue to miss deadlines because we just don't have the staffing to be able to carry through on all of the efforts required under the AML Act. The second is we are making tradeoffs. We are making tradeoffs against resources that can be used to engage in enforcement and compliance work that can be used to ensure implementation of our whistleblower program, that can be used to track ransomware actors, and to be able to support law enforcement, and to perform all of the other activities that we are doing and are required to do under the BSA.

Mr. CLEAVER. I am paranoid about the whole cryptocurrency issue, and I think I am going to remain paranoid for some time. In November of 2021, a FinCEN advisory on ransomware and the use of the financial system to facilitate ransom payment noted that cybercriminals usually require ransom payments to be denominated in convertible virtual currency, most commonly in Bitcoin. However, they are also increasingly requiring or incentivizing victims to pay an anonymity enhanced cryptocurrency. Now, what is the incentive for malicious actors to demand payment in an anonymity-enhanced cryptocurrency? I am presuming they believe they are maximizing their chances for getting away, for escaping.

Mr. DAS. That is correct, Congressman. I think that anonymity-enhancing currencies is another way in which ransomware actors and other criminal actors are working to avoid the financial system, and evade the financial system, and to hide illicit transactions. Again, we are very focused on ransomware. We have taken a number of enforcement actions with respect to cryptocurrency exchanges that support ransomware actors, and we are doing our best on this front.

Mr. CLEAVER. Thank you very much.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Missouri, Mr. Luetkemeyer, is now recognized for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman, and welcome, Director Das. You and I have had multiple conversations over the last few weeks about independent ATM operators, and today, I would like to put a few facts on record and discuss this issue with you again.

The fact is, for years the members of the Federal Financial Institutions Examination Council (FFIEC)and FinCEN supported the

notion that independently-owned ATMs are at high risk for money laundering. This was evident in the FFIEC BSA/AML Examination Manual, which contains many disparaging remarks about the industry and the so-called risk they pose to money laundering. Because the members of the FFIEC took the stance that financial institutions for the last several years have been refusing to provide financial services to independent ATM operators. However, because of the extensive conversations I have had with you and members of FFIEC, it has been determined and acknowledged that independently-owned ATMs do not, in fact, pose a high risk of money laundering. This became apparent when after multiple bipartisan meetings with Members of Congress, FFIEC changed its examination manual to accurately portray that independent ATMs are not inherently at risk for money laundering. In addition, I directly asked representatives of the FFIEC whether independent ATMs are a high-risk industry, and each of them individually said no.

Despite the changes made to the examination manual, I still hear reports of financial institutions cutting off access to services for independent ATM owners. That is because the regulators, the examiners for years have intimidated financial institutions into eliminating services to illegally-operating industries. The perception is still there, similar to an Operation Choke Point activity. It is now up to you and them to fix it, Director Das. That is why I am calling on all the prudential regulators and FinCEN to issue a policy statement to all financial institutions clarifying that independently-owned ATMs are not a high-risk industry for money laundering.

One excuse has been that we will be setting a precedent. This is not a precedent. In 2020, the agencies and FinCEN issued a fact sheet to all FDIC-insured institutions about nonprofit organizations (NPOs). Specifically, this fact sheet stated that, "NPOs do not present a uniform or acceptably high money laundering terrorist financing risk."

Mr. Chairman, I ask unanimous consent to enter into the record the document dated November 19, 2020.

Mr. HIMES. Without objection, it is so ordered.

Mr. LUETKEMEYER. Thank you. The reason I am bringing this all up today is I want to get these facts on the record of what has actually been going on with some of these agencies. They made up the charge that the money laundering was going on. They got caught, and now they need to fix it. And part of that fix is to fix the manual, which they have already done and are working on with the industry itself, and I applaud those efforts. The second part of it, though, is to clear up the perception that is still there with the financial institutions that this is a high-risk industry, and that these banks, if they want to go back and finance them, can do this again without punitive action taken by the regulators if they do it in a prudent, risk-free manner.

My question to you is very simple: Will you join the other agencies and send a statement clarifying that independent ATM operators do not have a high risk of money laundering?

Mr. DAS. Thank you for that question, Congressman Luetkemeyer, and I appreciate the conversations that we have had over the past weeks on this issue. Again, we agreed that this is an ongo-

ing issue in terms of clarifying the scope of this issue for examiners and for financial institutions as well. We are working with the banking agencies and the specific agencies to clarify this issue and to issue a joint statement, and we would join any such joint statement with the Federal banking agencies.

Mr. LUETKEMEYER. I thank you for that. I take that as a yes. In the future, I would just make the comment that your Agency should be a check on these other agencies to make sure this doesn't happen again. You should be pushing back on them when they do things like this, where there is no evidence that there was money laundering going on. Can you be a watchdog on that?

Mr. DAS. We will continue to engage with the banking agencies and to ensure that the record is clear on this point in terms of no particular customer type, including independent ATMs, present any automatically higher risk with respect to money laundering, correct.

Mr. LUETKEMEYER. Thank you very much for that. My time is about up. I have some more issues to discuss, expansion of some of the definitions with regards to benefit ownership rules and regulations, but we are out of time.

With that, I will yield back the rest of my time, Mr. Chairman. Thank you.

Mr. HIMES. The gentleman yields back.

The gentleman from New York, Mr. Meeks, who is also the Chair of the House Committee on Foreign Affairs, is now recognized for 5 minutes.

Mr. MEEKS. Thank you, Mr. Chairman. Good morning, and as indicated, I am the Chair of the House Foreign Affairs Committee, but I am also a member of this committee. And one of the issues that pops up now on both of our committees is dealing with Russia's illegal and immoral invasion of Ukraine. All of us have come together on both committees to impose significant sanctions on Russia and Russian oligarchs. As always, when it comes to sanctions, we are worried about how the sanctions can be circumvented, and sanctions have traditionally been scouted through shell companies in real estate, for example. And in FinCEN's March guidance, it is noted that the United States needs to also look out for the Central Bank of Russian Federation using import or export companies to engage in foreign exchange transactions on its behalf. Can you explain how FinCEN is monitoring these specific types of traditional means of sanction evasions, and what are some of the persisting issues that FinCEN is seeing with these techniques, not only as it relates to Russia, but also other sanctioned countries?

Mr. DAS. Thank you, Congressman. Our team has been working incredibly hard since the Russian invasion of Ukraine, on both the sanctions efforts and law enforcement efforts. We have worked incredibly hard to raise awareness on the part of financial institutions—that is, banks, cryptocurrency exchanges, and other financial institutions as well—about Russia's abuse of the financial system and their efforts to evade sanctions. We have issued two alerts so far: one on sanctions evasion specifically; and one on the efforts of Russian oligarchs to evade sanctions more generally and to hide their illicit assets, so that we can ensure that financial institutions

understand the ways in which Russian actors might abuse the financial system.

We also recently issued an advisory on cryptocracy as well. Those advisories and alerts alert financial institutions in terms of the red flags of either sanctions evasion or typologies with which Russian actors, oligarchs, proxies, and elites seek to evade sanctions. This allows financial institutions to better understand what types of transactions bad actors might engage in to evade sanctions. We have also reached out to financial institutions and to law enforcement across-the-board. This includes the FBI, the Department of Homeland Security Investigations (HSI), and the Department of Commerce's Bureau of Industry and Security, with respect to export controls, and others to participate in FinCEN exchanges with financial institutions so we can exchange information with financial institutions and law enforcement so that we can understand how to better trace and identify Russian sanctions evasions efforts, so we can get quality suspicious activity reporting from financial institutions that is actionable and that we can provide back to law enforcement as well.

We are very active in terms of reviewing the suspicious activity reports that we get, and we take those suspicious activity reports and distill those reports into summaries for law enforcement to use, and for OFAC to be able to use in their sanctions designations efforts and their targeting efforts as well. So, we have a number of different fronts, in terms of both working with financial institutions to collect more information in terms of trends or typologies of sanctions evasion, and then to take that information and translate it for OFAC and law enforcement to be able to use that information to go after Russian oligarch assets and to be able to identify other bad actors for sanctions designations as well.

Mr. MEEKS. Thank you for that. And I really can go deep, but I have another question, because you mentioned crypto, and I heard also conversations from Congressman Cleaver. We all have certain concerns about crypto. I am trying to find that balancing act, because I see there are some good purposes of it, and some people who try to utilize and get around have been concerned about Russia trying to use crypto to evade sanctions also, specifically. My question in the little time that I have is, is FinCEN thinking about new ways to implement Anti-Money Laundering/Know Your Customer (AML/KYC) procedures in this evolving world in a way that strikes a balance, and I want to know, what is, "to strike a balance?" And can you explain what FinCEN is already seeing with respect to crypto being used to evade sanctionsc, in 2 seconds?

Mr. DAS. I appreciate the question. As part of one of the alerts that we issued at the outset of the Russian invasion of Ukraine, the alert on sanctions evasion specifically highlighted the risks of cryptocurrency being used to evade sanctions. Again, we have not seen large-scale evasion through the use of cryptocurrency, but we are mindful of that and we are working with financial institutions so that they are aware of that potential so that we can identify a large-scale evasion using cryptocurrency and act on it as well. So, thank you.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Kentucky, Mr. Barr, is now recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman. Thanks for holding the hearing. Mr. Das, again, thank you for appearing here, and let me pick up right where Chairman Meeks left off on these advisories and alerts on Russian sanctions evasion efforts. I appreciate that FinCEN is issuing these advisories and alerts for law enforcement for financial institutions. I appreciate the communications between your Agency and law enforcement. But, Acting Director Das, can you go into a bit more detail about the data analytics that your Agency engages in, in providing that to OFAC? And can you give us a little bit greater granular detail about the analysis that FinCEN provides to OFAC to give OFAC the tools to thwart these sanctions evasion efforts?

Mr. DAS. I appreciate that. We do a number of different things on the analysis of information that we get with respect to Russia sanctions. First of all, we receive suspicious activity reports. We review those reports. We have reviewed over 2,000 Russia-related SARs, and we have referred 271 of them for further action to OFAC and to law enforcement as well. We have sent these reports to the FBI, and to the Department of Commerce's Bureau of Industry and Security as well.

Mr. BARR. Do you know whether or not OFAC has acted upon those 271 SARs that you have flagged for them?

Mr. DAS. We have provided OFAC with a substantial amount of information, either directly or through the Office of Intelligence and Analysis at the Treasury Department. We are aware that they review that information very carefully and they have acted on that information in the context of their designation—

Mr. BARR. Did they report back to you, hey, this has been helpful, we have now closed a sanctions evasion loophole or effort?

Mr. DAS. We remain in close communication with OFAC. We are part of a working team in terms of ensuring that OFAC has the information that we are seeing, and that we can engage with OFAC in terms of the sanctions designation and how they are using it. The short answer to your question is, yes, they do use our information. It has been used in sanctions designations, both in the context of Russia and in many other contexts as well.

Mr. BARR. Okay. Great. Keep up the good work there. FinCEN is asking Congress to authorize a sixth special measure, which would allow you to block fund transfers on a transaction-by-transaction basis, including for digital assets. However, special measures 1 through 4 appear to be rarely used, and FinCEN has often rescinded proposals to impose the fifth special measure against foreign financial institutions. Less than 2 years ago, you voluntarily withdrew a fifth special measure designation against Banco Delta Asia, which had been tied to North Korean money laundering. Why should Congress grant FinCEN a new sixth special measure to go after digital assets when the effectiveness of the first 5 special measures is unclear?

Mr. DAS. Thank you for that question. Again, we are very focused on the use of our Section 311 authority, as well as the authority in Section 97.14 of the NDAA from 2021, which includes a special measure sixth. Again, Section 311 was enacted in a time when

most financial relationships and transactions were done through the traditional banking system, where there are traditional correspondent account relationships. Nowadays, cross-border transactions often include money services businesses, payment systems, and well foreign exchange houses, as well as cryptocurrency.

So if we were to use the Section 311 authority against, for example, Chinese ransomware actors, those using dark markets and the like, we would not be able to use the Section 311 authority with respect to those transactions to prohibit those actors from abusing and engaging in money laundering with respect to the U.S. financial system. Currently, the Section 311 authority is not the right size for the types of threats that we are seeing through the use of cryptocurrency.

Mr. BARR. One final question. I do want to echo the concerns of the ranking member on FinCEN's development of its beneficial ownership database, and I want to highlight the leak of the SARs by a FinCEN employee. You talked about no hacking, that there has been no hack, but there was this very troubling report of a FinCEN employee in 2017–2018, as well as ProPublica's recent disclosure of details from a leaked IRS document. Data security looks to be not just a FinCEN problem, but a Treasury problem. What specific steps have you taken to ensure that these illegal disclosures never happen again?

Mr. DAS. When that disclosure happened, we referred the matter both to our Inspector General's office as well as to law enforcement. That individual was removed from the premises, detained, prosecuted, and served time. We are very focused on that. We took a number of steps in terms of the mechanism used by that individual in terms of being able to use a thumb drive. Thank you.

Mr. HIMES. The gentleman's time has expired.

Mr. DAS. Sorry. Very quickly, to use a thumb drive. We have ceased that use except under limited circumstances. And again, we have a robust internal security program to ensure that the database is used properly.

Mr. BARR. Thank you.

Mr. DAS. Thank you.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Colorado, Mr. Perlmutter, who is also the Chair of our Subcommittee on Consumer Protection and Financial Institutions, is now recognized for 5 minutes.

Mr. PERLMUTTER. Thank you, Mr. Chairman, and if my Wi-Fi goes out, just move on to the next participant here.

I would like to first thank Director Das for his service to our country at a very difficult time when sanctions have been imposed in many different ways against Russia, and obviously, the role of FinCEN has really grown by leaps and bounds as we deal with them. The ranking member talked about how you have massive amounts of information coming to you, and compared to what the normal person has, I would say that is true. But as compared to the Big Tech companies and other major institutions, you get a fraction of the information that they vacuum up every day. I just want to let the record reflect that, as massive amounts of information has to be compared to what and what.

Several of us visited the Caribbean recently and one of the things that came up again and again was money laundering issues, de-risking issues, and what appeared to be kind of redlining of that entire region, which has left the correspondent banking services to the Caribbean in really pretty sad shape. With the exception of Wells Fargo, it appears that correspondent banking has pretty much left the Caribbean. And so, I would like you to talk about, is FinCEN, is our ability to do the money laundering and Know Your Customer, can we do that on a nation-by-nation basis, or do you guys look at regions, or how does that work?

Mr. DAS. Congressman Perlmutter, thank you for that question and for the opportunity to discuss this topic. Again, financial inclusion and de-risking is incredibly important to FinCEN and to Treasury writ large. It is critical that countries, jurisdictions, and customers have access to financial services. De-risking is a real problem, and we are aware that it has impacted a variety of customers and sectors. There has been a lot of work that we have done to understand the root causes of de-risking, to identify what more that we can do on this front. And, in fact, the AML Act, under Section 6215, requires that we identify and develop a strategy to be able to respond to de-risking, and we have contributed to the GAO report on de-risking as well that was also required by Section 6215. Again, it is clear that the root causes for de-risking are complex, and that they really come down to the cost-benefit considerations and calculations that financial institutions are making when they decide with whom to do business. Some of these considerations are commercial and focus on business strategy and profitability.

It is also very important just to note that there are considerations that are related to jurisdictions' implementation of their AML/CFT rules in ensuring that they have robust AML/CFT frameworks within jurisdictions. We at FinCEN and at Treasury engage on a regional basis and on a country-by-country basis to ensure that countries are implementing high and robust AML/CFT standards as well. And to be able to encourage them to do so, we work through a number of different institutions as well, including the Financial Action Task Force (FATF), to raise standards and to ensure that countries are able to implement those standards, and that will provide confidence to financial institutions that they can continue to bank customers within specific countries and jurisdictions.

Mr. PERLMUTTER. Let me stop you for a second.

Mr. DAS. Yes.

Mr. PERLMUTTER. Let me stop you for a second because it appeared to us that there really wasn't a case-by-case or country-by-country kind of review of this, and not in a very frequent fashion, that there was just sort of this carte blanche against this region and really has affected individuals, and companies, and businesses down there because they can't get correspondent banking, and it has made it very difficult. I appreciate the general approach you take, but let's say with respect to this region, are you updating on a pretty continuous basis whether you think you need more de-risking or everything is okay?

Mr. DAS. Congressman, thanks for that question. With respect to specific details about how Treasury is engaging, particularly in the

Caribbean region, I am happy to follow up on that and provide you specific answers to your questions.

Mr. HIMES. The gentleman's time has expired. The gentleman from Texas, Mr. Williams, is now recognized for 5 minutes.

Mr. WILLIAMS OF TEXAS. Thank you, Mr. Chairman, and thank you for being here today, Mr. Das. When the Bank Secrecy Act was updated in the 2020 NDAA, the small business community expressed serious concerns about burdensome new regulations that would accompany this law. And Congress intended to strike this balance between tracking down bad actors within the financial system without hurting small businesses by directing your Agency to only collect four simple pieces of information. However, in the proposed rule, FinCEN is requiring businesses to report more information than is required by statute. Can you explain this decision and also shed some light on your communications with financial institutions as you have been developing these new regulations?

Mr. DAS. Thank you very much for that question, Congressman Williams. We are very mindful of the impact that the AML/CFT framework and the rules that we have to implement have on small businesses and the business community, more generally. In the context of the Beneficial Ownership rule, again, we are required to develop a beneficial ownership framework that is highly useful to law enforcement, while at the same time minimizing the costs and burdens to small businesses, and we are very mindful of that fact. We received a number of comments in the rulemaking process about the burdens that small businesses will face. We are taking into consideration very seriously those comments in the context of working towards the final rule as well.

Mr. WILLIAMS OF TEXAS. Yes, that is important, because small business is the heart of our economy, and they are getting buried right now. Everybody says I am for small businesses, but they add more regulations to what they need to do, so thank you for looking at that. And to keep on the topic of small businesses, the proposed rule estimates that there will be over 2.5 million new covered entities under this rule. For many of these businesses, this will be the first time that they have ever heard of FinCEN, and additionally, many will be wary of turning over their information to a new government agency, like most of us are. Again, how will you build trust within the small business community as well as educate them on what will now be required of them?

Mr. DAS. Thank you for that question. As we work through the rulemaking process, with respect to all of the three different rules that we have to issue in the context of the Corporate Transparency Act, we are planning an outreach process to reach out to industry groups, to financial institutions, to State-level secretaries of state, and others to be able to ensure that the business community, stakeholders, and individuals across America understand what the rules do, what they require of small businesses and others within in terms of reporting, and we plan on proactively engaging. This requires an extensive strategic plan.

And again, when it comes back to resources, this is part of the reason that we are asking for additional resources to be able to support our FTE hiring so that we have the people available to develop an outreach strategy, to implement that outreach strategy,

and to engage with a high number of industry groups, again States and secretaries of states, businesses, and to do the type of stakeholder outreach that we need to do to ensure that everybody understands the scope of the rules, what they are required to do, and how that information is going to be used.

Mr. WILLIAMS OF TEXAS. Small businesses are scared to death of new government agencies, and when you start talking about hiring more, hiring more, that really worries small businesses. I am a small business owner, and I hear what you are saying, but it is worrisome. We have heard about the massive inflow of CTRs and SARs coming into the Agency. One solution that many of my Republican colleagues and I have advocated is to raise the monetary thresholds to file these reports.

As a reference point, when this law was first adopted in the 1970s, a brand new Corvette—I am in the car business, so I measure by this—a brand new Corvette sticker price was $5,000. Today, the same model car costs over $100,000. And even with this huge increase in prices, the thresholds to file these reports has stayed the same. So, I do not see how you can effectively recognize bad actors when they are being obscured among the hundreds of thousands of other reports that are filed. Another question, how do you think we can make the reportings regime more effective so FinCEN is receiving fewer overall reports from the financial institutions?

Mr. DAS. Thank you for that question. Again, Section 6204 and Section 6205 of the AML Act require us to review the reporting thresholds for currency transaction reports (CTRs) as well as suspicious activity reports. That is something that we are currently undertaking. We are engaging with a number of other agencies at the State and Federal level in terms of understanding the use of the report and a number of proposals in terms of both raising the thresholds as well as considering lower thresholds in terms of developing what is most useful for law enforcement. That is an ongoing review. We also intend to sort of link up that review with our review of information coming in through Section 6215—

Mr. HIMES. The gentleman's time has expired.

Mr. WILLIAMS OF TEXAS. I yield back. Thank you.

Mr. HIMES. The gentleman from Illinois, Mr. Foster, who is also the Chair of our Task Force on Artificial Intelligence, is now recognized for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman, and thank you, Acting Director Das, for your service in a very challenging time. And I also have to say, as a former and successful small business owner myself, I share my Republican colleague's enthusiasm for the role of small business, and I hope that we can both applaud, on a bipartisan basis, the record number of startups that are happening under President Biden's economic recovery.

Now, I understand that FinCEN has had notable success in combating some classes of illicit cryptocurrency cases through either blockchain analysis or through other more traditional detection methods. I presume that you have also been mostly successful in preventing illicit crypto use in transactions involving exchange accounts or hosted wallets that comply with AML/KYC standards. However, I worry that we are much less equipped to handle in-

stances where transactions involve self-hosted wallets or generally off-exchanges.

In a hearing a few months ago in this committee, when we had several crypto industry leaders, they acknowledged that if we wish to prevent crypto from being used for ransomware and other illicit payments, that there is no alternative to having all crypto transactions pseudonymously attached to a legally-traceable, secure digital identity from a country with which we have extradition treaties. And this is something that they acknowledged was sort of a logical necessity here.

In late 2020, FinCEN proposed a rule that would amend the implementation of the Bank Secrecy Act regulations and require banks to provide KYC information and digital asset transaction records for unhosted or self-hosted digital wallets. However, if we end up with a regulatory regime where bank accounts are not needed to create or access a digital wallet, what might the regime that works to prevent money laundering, ransomware, and so on—how would you monitor something like KYC compliance if it is not tied to a bank account?

Mr. DAS. Thank you for that question, Congressman Foster. In terms of the rule, first of all, for the NPRM that was issued in 2020, a number of comments were made. I think we received over 8,000 comments to the NPRM. We are reviewing those comments and considering next steps in terms of the overall approach. With respect to the risks presented by unhosted wallets, again, it is not that unhosted wallets are entirely opaque. Unhosted wallets often engage in transactions with cryptocurrency exchanges, which are subject to AML/CFT regulation, and those are subject to SAR reporting requirements as well. Law enforcement can engage with cryptocurrency exchanges with respect to suspicious activity reporting and other reports that might be applicable to them in terms of getting some degree of understanding in terms of transactions with unhosted wallets as well.

Mr. FOSTER. Yes, but there are limits to that, which we probably shouldn't talk about here, but there are limits to your ability when you start to use privacy-enhanced coins when you go through multiple devices designed to obscure the origin of transactions in them.

Mr. DAS. And that is something that we are very concerned about. Again, the illicit finance risks of transactions that are not transparent create significant illicit finance risks, and that is something that we are very focused on in the context of understanding more effectively the cryptocurrency industry and how cryptocurrencies use this to be able to better assess what those channels of illicit finance risk are, and to be able to find ways to identify an appropriate regulatory regime so that appropriate AML/CFT controls are in place. But again, this is a question that we are very focused on with respect to unhosted wallets as well as other types of convertible cryptocurrencies.

Mr. FOSTER. Yes. I think ultimately, it seems like what you are going to need is some sort of an internationally-operable crypto driver's license that you attach to every crypto transaction, that you can use. When you see a crime has been committed, for example, you can go to a trusted court system and get that deanonymized and find out when your screen locks up with

ransomware, you have to be able to go to a judge and say, here is the proof that a crime has been committed, and I want to know who owns that wallet. And to have the judge in a trusted jurisdiction is an important part. And that seems to only work if you have something like a crypto license attached pseudonymously to every transaction. I don't see a logical alternative to that. And if you are aware of one, I would be very interested as you interpret all of these comments coming in.

Mr. DAS. I appreciate that, and that is something we can follow up on with you.

Mr. FOSTER. Thank you.

Mr. HIMES. The gentleman's time has expired. The gentlewoman from Missouri, Mrs. Wagner, is now recognized for 5 minutes.

Mrs. WAGNER. Thank you, Mr. Chairman. Good morning, Acting Director Das. As you are aware—and I do appreciate your meeting with me and my staff—the pandemic caused a horrific spike in the amount of child sexual abuse material (CSAM) found online. In 2021 alone, the National Center for Missing and Exploited Children received nearly 30 million reports of online child sexual exploitation, which is a staggering 70-percent increase in this illegal, illicit exploitation from 2019.

The financial sector plays a vital role in combating the distribution and sale of these disturbing images and videos of children being sexually abused, but clearly, much more needs to be done. Title 31 of the U.S. Code requires the financial sector to implement effective anti-money laundering compliance controls. Combating human trafficking, including crimes against children, is one of FinCEN's anti-money laundering priorities.

I would like to submit for the record, Mr. Chairman, two reports compiled by separate anti-trafficking organizations using different investigatory methods, both of which found extremely troubling results on a website that also grew massively during the pandemic, and that is known as OnlyFans.com.

Mr. HIMES. Without objection, it is so ordered.

Mrs. WAGNER. I thank the Chair. Currently, major U.S. credit card companies must comply with Title 31 regulations to allow their products to be used to purchase content on this website. Although there is no legal issue with purchasing content involving consenting adults, this report by the Avery Center found, "A clear correlation between third-party traffickers and minor victims on OnlyFans." And the platform has, "no screening procedures to identify situations where exploitation or abuse are occurring."

The other report by the Anti-Human Trafficking Intelligence Initiative and the University of New Haven found again, "A high value of OnlyFans profiles possessing commonly understood indicators of CSAM—again, CSAM is child sexual abuse material—and sex trafficking within less than 2 hours." These reports assert that the U.S. financial sector is enabling this illegal commerce by, "failing to adequately comply with their existing regulatory requirements mandated by Title 31."

Acting Director Das, what are the regulatory requirements that credit card companies must comply with in order to prevent the use of their products to purchase CSAM and non-consensual sexual imagery?

Mr. DAS. Thank you for that question, Congresswoman Wagner. Again, credit card companies are subject to defined AML/CFT program requirements under our rules where they need to focus on whether or not their partner financial institutions are engaged in money laundering or terrorism financing. However, in the overall framework, credit card companies act as intermediaries in the overall financial system in terms of payments between merchants and financial institutions. The financial institutions at the end that deal with customers who might be malign actors are required to file suspicious activity reports when they see information that they may suspect is linked to illicit finance activity. And the financial institutions do file suspicious activity reports in relation to online child sexual exploitation.

Mrs. WAGNER. I know that we are going to run out of time, and I just want to thank you and your office for working with me. And I would implore my colleagues on the committee to also get on board and work with our office in this regard. More has to be done to ensure that this child sexual abuse material cannot be purchased using mainstream financial tools like a credit or a debit card. So, I am imploring my colleagues and FinCEN to work with me to find a solution to keep our children safe; A 70-percent increase during the pandemic is unacceptable.

I thank you, Director Das, for your support on this, and I appreciate the Chair giving me the indulgence of time, and I yield back.

Mr. HIMES. The gentlewoman's time has expired. The gentlewoman from Ohio, Mrs. Beatty, who is also the Chair of our Subcommittee on Diversity and Inclusion, is now recognized for 5 minutes.

Mrs. BEATTY. Thank you, Mr. Chairman, and thank you also, Acting Director Das, for being here today. I have a two-part question, but, first, for the record and for the sake of time, I won't repeat Congressman Perlmutter's question. But I, too, was on that same CODEL with him, and I also want to associate myself with the words of Congressman Foster.

With that said, Mr. Das, what we heard, and I will say it a little differently, as Mr. Perlmutter referenced being redlined—we heard this repeatedly from heads of states to the point that they felt they were being punished by United States secretaries of states in how our process works as it looked to blaming them for money laundering or blaming them for crimes that they didn't believe were necessarily the case. We all understand it is a delicate balance, but I guess I, too, share a concern that these are people of color, and they were a lot stronger than the redlining. They thought part of it dealt with systemic racism. And I made a commitment, like the others on the CODEL, that we would come back and really take a look at this. I would like to join you in that dialogue when you have it with Mr. Perlmutter.

But let me also say, like most of us, or all of us rather, I represent people who are amongst the 9 million Americans who live abroad. And one of those constituents by the name of Rebecca emails my staff frequently. She lives in England, and she raised this issue with us specifically for this hearing. And it has to do with FinCEN Form 114, the Report of Foreign Bank and Financial Accounts, or FBAR, which people are required to file, as you know,

if they have aggregate foreign holdings of over $10,000. And for a lot of people living abroad, the FBAR is another confusing form on top of the special reporting that they also have to do to the IRS. Now, as I understand it, the $10,000 threshold hasn't been updated in decades, and I think the BSA was sometime around 1970. And since it is aggregate, once you have assets above that amount, you have to file the information on all of your accounts, regardless of how small they might be.

Now, I want to be clear again, I don't want to advocate for anything that impedes your ability to weed out money laundering or any type of illicit financing, but at the same time, my question is, is it worth us taking a look at making an adjustment to that? If you would look at inflation over the decades since it was established, from $10,000, if I wanted to do legislation to say, take it to $70,000, accounting from the 1970s to the present, is that something that you could support?

Mr. DAS. Thank you very much for that question, Congresswoman Beatty. I think the answer is that we would review the thresholds for FBAR reports as well. I think it is an important issue to review, and, in fact, we are in the context of Section 6204 and Section 6205 of the AML Act. We are reviewing the thresholds with respect to CTRs as well as with respect to SARs.

In the context of Section 6216 of the AML Act, we are also reviewing, more generally, the effectiveness of the reports that we receive, and in that context, I think it is important to review the thresholds with respect to FBARs. But I would like to say that FBARs are incredibly important to law enforcement, and they are incredibly important to the IRS as well. Some law enforcement agencies, particularly those investigating tax-related crimes such as the IRS CI, work mainly with FBARs and/or the absence of FBARs to be able to generate cases. And they use the account and ownership information to generate cases and to target tax evaders and the like.

Mrs. BEATTY. My time is almost up. Mr. Director, let me just say this because the clock is running out. I think I hear you, and I get the gist of it. I am not trying to impede them. I am just saying, let us take a look at the $10,000, keep the same rules, but let us lift the bar.

Mr. DAS. We can take a look at that.

Mrs. BEATTY. Thank you. And thank you, Mr. Chairman.

Mr. HIMES. The gentlelady's time has expired.

The gentleman from Arkansas, Mr. Hill, is now recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman. I appreciate you being the Chair. I join with the ranking member in wishing Chairwoman Waters a speedy recovery from COVID. Nobody's family has suffered more than hers, losing her sister very early in the pandemic. And thank you, Acting Director, for being here today, with very helpful testimony.

Would you be willing to come once a year and visit with the committee on behalf of FinCEN?

Mr. DAS. Of course, yes.

Mr. HILL. Thank you. That would be very helpful. I think we were all so pleased with your briefing the other day. We just don't

have access to this level of detail, so I think it is very helpful to Members. Mrs. Beatty raised the issue of thresholds. Others did as well. I just would remind the Acting Director that neither Secretary Lew nor Secretary Mnuchin were particularly forthcoming or helpful in trying to review or raise those thresholds. We had bipartisan bills here, I think, Mr. Himes, for three Congresses that would have done some modest inflation adjustment of the CTR and SAR threshold. So, I am glad to hear you are going to look at them, and we would welcome Secretary Yellen being a more forthcoming interlocutor on trying to raise those somewhat without impeding law enforcement. I think that is possible. Would you agree?

Mr. DAS. Again, Section—

Mr. HILL. Don't repeat the section numbers. Just, do you agree or not agree? Do you agree that raising the thresholds is a possibility and might be beneficial to both sides?

Mr. DAS. We are looking at a number of proposals with respect to raising thresholds and seeing what the impact will be.

Mr. HILL. Yes, okay. Good. I appreciate that. Have you done a cost/benefit analysis at Treasury using your great macro resources on the new Corporate Transparency Act proposal for beneficial ownership?

Mr. DAS. The reporting rule, NPRM, that we published last December includes a regulatory impact analysis that includes evaluation of what the costs would be to business, yes.

Mr. HILL. When it was proposed, I was very opposed to this style. I am not opposed to improving beneficial ownership, but I was very opposed to Mrs. Maloney's bill. I worked very hard against it and offered alternatives. Again, our mutual good friend, Secretary Mnuchin, didn't agree, nor did the Chair of the Ways and Means Committee, so I lost out on my approach. But I think you are going to find this is going to be one of the most expensive regulations ever imposed on American business, so I want to associate myself with Mr. Williams' comments.

And just in the last 16, 17 months of the Biden Administration, the American Action Forum has released that the Administration's regulatory costs in the economy are up about $200 billion annualized from the Trump level, so we are all very sensitive to the imposition and cost of regulations on our small businesses.

And I think Mr. Williams summarized some of the concerns we have about the beneficial ownership rule. Would you be willing, when you get ready for that notice for final rulemaking, to brief and receive some final comments, not approval, we understand separation of powers, but some final comments from Ranking Member McHenry and Chairwoman Waters, because I know they have divergent views on this. That makes it hard on you. We recognize that, but would you be willing, before that rulemaking is published, to visit with Ranking Member McHenry about it?

Mr. DAS. Thank you for that question. Again, we are subject to APA requirements with respect to notice-and-comment rulemaking. To the extent that, from my perspective, from a FinCEN perspective, we are happy to brief you on the rules and the contours of the rules as well, but it would have to be subject to the notice-and-comment rules and we would have to follow those rules in terms of any—

Mr. HILL. Let's think about that, because we are concerned about the cost of this rule. Let me shift comments and talk about the topic really of the day for Mr. Himes, Ms. Waters, Mr. McHenry, and all of us, and that is what we are doing to track down Russian oligarchs. You were very helpful and forthcoming the other day in our briefing, but of course, we have sanctioned Russia, and Russian people, and Russian entities, particularly since the Crimean invasion back in 2014. And you cited the SARs and the possible connection of SARs, 271 out of 2,000 that were referred to law enforcement. Let me narrow that a little further and ask you, since 2014, are you aware of a prosecution of a Russian connected to sanctions evasion that was related to a SAR filed in the United States?

Mr. DAS. We have taken compliance efforts with respect to entities linked to Russian ransomware activities. In terms of a specific Russian prosecution with respect to sanctions evasion, I would have to refer you to DOJ on that question. And I am happy to follow up with you on any questions that you may have.

Mr. HILL. Yes, let's follow up on that. Thank you. I yield back, Mr. Chairman.

Mr. HIMES. The gentleman's time has expired. The gentleman from Illinois, Mr. Casten, who is also the Vice Chair of our Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets, is now recognized for 5 minutes.

Mr. CASTEN. Thank you, Mr. Chairman. Acting Director Das, it's nice to see you again. I want to follow up on a conversation you and I had a couple of weeks ago, specifically about the Deutsche Bank mirror trades in 2014 and the degree to which we have closed that barn door. This was, of course, the situation where Russians were executing simultaneous buy and sell trades to move rubles into hard currency. And when we talked about it a couple of weeks ago, I was thinking about it in the context of, if we close the barn door, Russia can't use that to either influence foreign politicians as they were using in 2014, or to get hard currency to prosecute their war crimes in Ukraine. It is, of course, back in the news this week with the news of Val Broeksmit's death, who was the whistleblower, who, among other things, disclosed what was happening at Deutsche.

What I would like to understand with you, from a FinCEN perspective is, do you have jurisdiction or do you receive SARs reports if a non-U.S. actor is laundering money through non-U.S. markets? I think the answer is no, but I just want to clarify that my understanding is right.

Mr. DAS. Your question is whether or not we receive SAR reporting when a non-U.S. actor launders money through non-U.S. markets, is that correct, sir?

Mr. CASTEN. Yes.

Mr. DAS. If there is a touchpoint to the U.S. financial system, and the financial institution is able to identify any illicit activity, we would receive a suspicious activity report. If the action is entirely outside of U.S. jurisdiction, and it doesn't have a touchpoint with respect to a U.S. financial institution, I am just struggling to see a situation in which we would see a suspicious activity report.

Mr. CASTEN. Okay. So if I understand it, FinCEN is a member of the Egmont Group, which is sort of trying to tie that with your

peers in other countries. Let's say a bad actor, not a U.S. flag, doesn't trigger a SARs report and they are in two other countries. Would you find doubt about it? Do you have jurisdiction? Can you put the appropriate walls up if that is flagged by one of your partners in the Egmont Group? Is that what the Egmont Group is intended to do? Do I have that right?

Mr. DAS. You have that right, Congressman. It would depend on a couple of different considerations. One is we have the ability to ask questions of our Egmont Group partners with respect to law enforcement actions or investigations that might be ongoing in the United States and to identify whether or not our counterpart FIUs might have that information. There may be some situations in which Egmont Group partners spontaneously disclose that information to FinCEN. And if they did disclose that information when they think that the United States might have an interest, we would review that information, and, if appropriate, pass it on to law enforcement agencies.

Mr. CASTEN. Okay. This is rapidly going to get into areas where this may not be the appropriate forum to discuss this, but let me just sort of walk through where my concern is, and you can comment as you see fit. We know from the mirror trading scandal that Deutsche Bank broke the law. They were fined. Thank you. We know that they were influenced to some degree by Russian money. They were tempted by the commissions. And we know that Russian money has been used to corrupt an awful lot of people in our world, sadly, and that is a part of what they have been using that laundered money to do.

As we now try to make sure that they don't have the resources to continue to commit these acts across cities in Ukraine, that all of our sanctions are effective, have we and our international partners sufficiently closed that down, or are we at risk that just one bad corrupted actor, one bad country can still provide the gap so that Russia could find their way through that and all of a sudden the money is into somebody whom we don't know about or some company that is not triggering any flags for us? Are we doing enough to close that down? Is this a U.S. law issue? Is it an international law issue?

And some of that gets well beyond the jurisdiction of this committee, but I would like to understand, as we impose these sanctions, so that we have a good understanding that they are actually going to affect the people intended and are, at the very least, consistent with where those gaps are in international. I realize it is a big, meaty question. I would welcome your comments and maybe continued conversation given the time.

Mr. DAS. I would be happy to continue the conversation with you. I think on our part, and in terms of ensuring that we understand how Russia is evading sanctions or abusing the financial system, we have actually set up a group with our counterpart FIU, our closest partners, for example, the U.K., the EU, Australia, and others, to be able to work together to identify key issues with respect to Russian illicit finance and to be able to exchange information quickly and on an effective basis to be able to support law enforcement and the intel community in terms of targeting exactly the types of activity that you are discussing.

Mr. CASTEN. Okay. Thank you, and let's have a follow-up conversation. I yield back.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Georgia, Mr. Loudermilk, is now recognized for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman. Acting Director Das, it's good to see you again. I would like to start off by discussing the implementation of the anti-money laundering and beneficial ownership reporting law. The proposed rule's definitions of, "substantial control," and, "ownership interests," are quite complicated, which would make it hard to apply them consistently. This problem is going to be compounded, in my opinion, for financial institutions if FinCEN uses those same definitions in an updated customer due diligence rule. My first question is, will FinCEN take steps to simply define these definitions before the rule is finalized?

Mr. DAS. Thank you for that question. The substantial control rule is a rule that is covered in the NPRM. We received a number of comments on the substantial control rule, the contours of it, the benefits that it might provide in terms of providing a highly-useful database for law enforcement, as well as some of the complexities in terms of implementation of that substantial control role. We are taking a hard look at those comments in the context of moving towards a final rule, and we will consider issues that were raised in the comments, including by a number of you in terms of the contours and the costs imposed as well.

Mr. LOUDERMILK. Okay. I would appreciate if you would keep us informed on the direction that you are going and the decisions that you make there. Another question is, the law requires FinCEN to minimize burdens on businesses, but it appears that FinCEN is not following that requirement. For example, FinCEN has expanded the scope of who is required to file, expanded the types of information that must be filed, and set very short compliance deadlines. My question is, are there examples in the rule where FinCEN has minimized compliance burdens, as the law requires?

Mr. DAS. We proposed a rule that would develop a highly-effective database for law enforcement to use. We evaluated the impacts that businesses and particularly small businesses would have. We estimated that the costs of the rule for small businesses would be at $45 per business for a filing, for the initial filing, which is comparable to the cost that small businesses would have to pay just to establish an LLC, which ranges anywhere from $40 to $500, depending on which State is involved in terms of incorporating it. Again, we received a number of comments around both the costs and the implications for small businesses as well as the complexity of the rules. We found the comments to be incredibly helpful and instructive, and we are taking all of those into account in terms of next steps as we work towards a final role.

Mr. LOUDERMILK. And I trust you will keep us informed on the direction that you are going, and again, as the law requires, minimize those burdens as much as possible. I would like to follow up on something that my colleague, Mr. Williams, discussed, and that is Section 6205 of the Anti-Money Laundering Act, which requires Treasury to conduct a rulemaking to consider changing the dollar

threshold for SARs and CTRs. This is badly needed because institutions are currently required to file more than 20 million CTRs and SARs every year, most of which have no value to law enforcement. In fact, a 2018 study indicated that 4 percent of SARs and 0.44 percent of CTRs warranted additional review from law enforcement. That is a very low number compared to the amount of data that businesses are required to report. What is the status of the reports and rulemaking required by Section 6205?

Mr. DAS. Could you repeat the question? I'm sorry.

Mr. LOUDERMILK. Okay. What is the status of the reports and rulemaking required by Section 6205? How are you going to modernize this reporting requirement?

Mr. DAS. We are working on the reports under Sections 6204 and 6205. We have engaged with all of the consulting agencies that are involved. We are reviewing a number of different proposals from a number of different sources. With respect to the CTR and the SAR reporting threshold, we expect to issue that report later this year in conjunction with the two reports together. And again, we are currently evaluating the issue. We are very focused in terms of priorities, given there are resource constraints on getting the beneficial ownership rule done and the real estate process moving forward as well. But this is something that we are actively working on, and we hope to get it done as quickly as possible.

Mr. LOUDERMILK. Thank you. I see my time has expired, so any other questions I have, I will submit for the record. And I yield back the balance of my time.

Mr. HIMES. The gentleman's time has expired.

The gentleman from California, Mr. Sherman, who is also the Chair of our Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets, is now recognized for 5 minutes.

Mr. SHERMAN. Thank you. Acting Director, when Secretary Yellen testified before us a few weeks ago, I asked about the time frame by which we can expect the beneficial ownership database to be established. As you know, that database is required under the Corporate Transparency Act, which passed in January of last year. Under the law, the database is supposed to be implemented within 1 year, so it is a few months late. Secretary Yellen pointed out that FinCEN has proposed one of the two rules that the Agency believes are necessary to establish the database. I know you are a few months late now. Can you give us some detail as to what is preventing you from meeting the timeline and, more importantly, when we can expect the database to be established?

Mr. DAS. Thank you so much for that question. Again, the Corporate Transparency Act requires that we issue three rules: first, a reporting rule that governs the information that is provided to FinCEN that goes into the database; second, the access rule, which provides the guidelines and rules for how law enforcement agencies and others access the database; and third, it requires us to issue revisions to the Customer Due Diligence (CDD) rule, which needs to be issued 1 year after the effective date of the reporting rule. As the Secretary mentioned, we are very focused in terms of the use of our resources in getting the access rule NPRM done by the end of the year, and we are working hard to do it. At the same time, in parallel, we are working on the comments to the reporting rule.

We received a substantial number of comments. It is an incredibly complex issue, and it is incredibly important for some of the reasons stated here today that we just get it right.

Mr. SHERMAN. Okay. Congress gave you a year to do it. You think it will take 2 years to do it. You are confident, or how confident are you that you will be able to get it done by the end of this year?

Mr. DAS. Again, we are committed to getting the access rule NPRM done by the end of this year.

Mr. SHERMAN. Will that then lead to the establishment of the database, or do you have to then do the revisions to the third rule?

Mr. DAS. I do not have a timeline for the establishment of the database. Again, we are working incredibly hard given the resource constraints that we have and the complexity of the issues.

Mr. SHERMAN. Okay. I will urge you to get this done as quickly as you can. It is important.

Mr. DAS. Again, we are very focused on getting it done as quickly as possible.

Mr. SHERMAN. When Secretary Yellen came before this committee last month, I highlighted a recently-published article in The Washington Post saying that yachts and mansions are easier for us to track down when we are going after the Russian oligarchs than interest in hedge funds and equity funds, venture capital funds, et cetera, because they are not required to disclose beneficial ownership information to you or to the SEC. In February, the House passed the America COMPETES Act, which included an amendment I offered, which would require issuers of exempt securities to file beneficial ownership information with the SEC with regard to large transactions.

Would you agree that increased Federal Government visibility into our $11 trillion private securities market, especially knowledge as to beneficial ownership, would help us combat the Russian oligarchs?

Mr. DAS. Thank you for that question. As we have noted in our unified regulatory agenda, we are actively considering a proposed rule that would address existing gaps in regulatory coverage for investment advisors, taking into account the comments that were submitted during the NPRM process that occurred in 2015. Again, we are working from a FinCEN perspective with Treasury's Office of Terrorist Financing and Financial Crimes in a number of different efforts to be able to better understand the risks presented by investment advisors as we think about what the appropriate rule might look like and what the scope and coverage might look like as well. In the meantime, we are very focused on this issue in the context of Russian illicit finance and the way Russian oligarchs are abusing the financial system. And again, we are working—

Mr. SHERMAN. Let me try to squeeze in one more question. We have sanctioned 400 individuals and entities, as well as, of course, the Russian government. The crypto world is not big enough to handle the major governmental transactions, but they are big enough for some of the oligarchs. We hear that the crypto industry transactions is a technology which would allow for traceability. However, privacy coins, like Monero, and protocols, like Lightning

Network, can be effective in obscuring transactions. How focused is FinCEN on looking at crypto at the oligarch level?

Mr. DAS. We are focused on it. Again, we issued a sanctions evasion alert around potential evasion using cryptocurrency. And again, we are very focused on this issue in terms of trying to identify means through which cryptocurrency might be used to evade sanctions or to bolster the Russian economic system as well.

Mr. SHERMAN. Thank you.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Ohio, Mr. Davidson, is now recognized for 5 minutes.

Mr. DAVIDSON. I thank the chairman, and I thank Acting Director Das. Thank you. Thank you for your time and, frankly, taking the time to meet individually with some of our Members, including me and my staff. We appreciate the challenge that you are up against.

As Mr. Hill highlighted, I have worked passionately and vigorously to stop some of the things you are working on, but they passed anyway, and so there is a law. I understand that you are implementing them. I do hope that we can make them less bad than they would potentially be. And I share some of the concerns that he, and Mr. Williams, and others have highlighted, so thanks for listening, and we hope that we can continue to collaborate as we go through this development process.

Today, I am in the process of introducing the Financial Crimes Enforcement Network Improvements Act, which would provide additional accountability. It would provide a path for your role as the Director to be a Senate-confirmed position and provide some of the things that you have personally been willing to do, like come before this committee and testify in an open setting, and also meet with us in a classified setting, because it is really important for our nation to have the world's best financial intelligence organization. I know that we have an advantage because we have the power and influence of the U.S. dollar, but we hope that advantages also not just great people, but great authorities for our FinCEN.

And when you look at how we go about, inherently in America in intelligence, we are also constrained in some ways that maybe more authoritarian regimes wouldn't feel hindered by, which is we need to protect civil liberties, and we need to do these things in a way that provides privacy and due process and is concerned about the impact on our economy. So, we probably disagree on what the costs are for compliance for small businesses.

But I highlighted another thing. Just recently, talking to the Congressional Budget Office, they thought that student debt was going to be better when the government operated student lending programs, and they said we were going to save $68 billion by taking over student lending. What we know is actually just in defaults alone, it is going to cost half a trillion dollars, so the financial modeling on all this is pretty bad. When we just have these debates and you say one thing, it is just words. When you look at the financial models, it is really just understanding what is it really like.

As a small business owner, as someone who spent a lot of time in the private sector, this is a very disruptive thing aside from the cost, because it assumes that the citizen somehow has to come to

the government to get permission to operate, and, in fact, that is exactly what my colleague, Mr. Foster, highlighted. Perhaps the most disturbing thing that I have heard is the idea that to access your own money, you need to get some identity, some globalist-conforming identity stamp, and then everything that you want to do is tracked and monitored. And then, when they want to rewind the tape and figure out who it was, they may not even need to get a warrant; they just come and expose who that person is.

I think that the way that we protect our way of life is by being less like China and more like America, because this is exactly what China is in the process of implementing. And when they hear the things that you are working on, people back home fear that what you are part of building is a system, frankly, a dystopian system where the average citizen needs to get permission to access their own money. And I think that is why the self-hosted, self-custody of crypto, basically if you download software and you use it, somehow you could become a criminal under this self-hosted rulemaking that has been proposed. Could you talk about self-custody and where FinCEN is headed with that?

Mr. DAS. Thank you for that. First of all, I entirely agree with you in terms of the importance of FinCEN's mission in getting it right. Second of all, we are very focused on privacy interests in the context of what we do. That is an important concern in terms of the information that we get, as well as how that information is used. Third, in terms of the self-hosted custody wallet rule, the unhosted wallets rule as we call it, and again, we received a number of comments. They raised a number of privacy considerations in those comments, both with respect to the unhosted wallets rule as well as the travel rule. We are taking a close look at that and reviewing it and our consideration of next steps.

Mr. DAVIDSON. I hope that the Keep Your Keys Act will feature prominently, which protects the ability of the ordinary citizen to continue to own digital assets and, frankly, self-custody. Thanks for the work, and I yield back.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Massachusetts, Mr. Lynch, who is also the Chair of our Task Force on Financial Technology, is now recognized for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. Thanks for holding this hearing. I want to thank our witness as well for his accessibility. As Mr. Davidson noted, Mr. Das has been very good with his availability.

I do want to ask, I look at the funding for FinCEN and I also look at the responsibilities that you have, and I know that despite the importance of the role that FinCEN plays, the current funding levels are about $430 million short of what we would recommend for your agency. And I am just curious as to how you work around that issue? Are there tradeoffs that have to be made? I know that Congress did make an additional appropriation in connection with the Ukraine situation. But where do we stand now and how are you doing that workaround where you don't have enough resources to hire the number of agents that would be appropriate given the scope of your responsibilities? Could you talk about that a little bit?

Mr. DAS. Sure. I appreciate that question about our budget. Again, we appreciate the funding that was provided under the Fiscal Year 2022 appropriations as well as the Ukraine supplemental. The Fiscal Year 2022 appropriations will in large part go to supporting our IT system, as well as our beneficial ownership database. The Ukraine funding will be used in a number of different respects to help support our analyst team in tracking and tracing funds related to sanctions evasion and illicit finance as well.

Where the Fiscal Year 2022 appropriations comes up short is with respect to funding to support hiring additional FTEs to be able to do all the work that we have to do. As a result, there are huge tradeoffs that are made in terms of our ability to engage in the enforcement and compliance work that our Office of Compliance and Enforcement does, to be able to ensure that financial institutions, cryptocurrency exchanges, and others have reasonably-designed and effective AML/CFT programs. It constrains our ability to get the rules and regulations done to implement the AML Act, and that is incredibly important because we are simply missing deadlines at this point. It constrains our ability to hire analysts, particularly in the cryptocurrency area, to be able to do the type of analytics that is required to understand how cryptocurrencies are flowing and contributing to illicit finance.

And our team is incredibly talented, but they are incredibly small as well, and they are just outmatched by the challenge, not in competence, but in terms of resources alone. And we continuously run up against challenges in terms of trying to figure out who is available to do work around cryptocurrency issues, to be able to combat that illicit finance. And again, we are constrained in our ability to engage in public/private partnerships and outreach forums like the FinCEN Exchanges and Innovation Hours, to be able to execute on the AML Act's directive to engage more with financial institutions so they understand how law enforcement is using the information that FinCEN has so we can provide feedback to those financial institutions in terms of what works and what doesn't work. And there are a number of different fronts in which we are just coming up short in terms of fulfilling what I think the AML Act intends for us to do, which is to create a robust framework.

Mr. LYNCH. Great. I only have another minute, and I do want to get another question in. With the advent of digital wallets, we have a whole area of vulnerability now. The New York Times just wrote a great piece about the vulnerability of these digital wallets, and 19 million Americans last year were scammed or had their money stolen on these platforms because of the vulnerabilities in these digital wallets. This is sort of a growing phenomenon. There is a big adoption rate, a very high adoption rate in the economy right now. Those are financial crimes. Does FinCEN have visibility on that new development? And tell me, how are you redirecting resources to that problem?

Mr. DAS. Cryptocurrency exchanges are subject to FinCEN's AML/CFT program requirements. They are required to file suspicious activity reports if there is any indication of a financial crime or if they reasonably suspect a financial crime. So, we would

have a certain degree of visibility if it filters through in our suspicious activity reporting.

Mr. LYNCH. Okay. Thank you. Mr. Chairman, I yield back. Thank you.

Mr. HIMES. The gentleman's time has expired.

The gentleman from West Virginia, Mr. Mooney, is now recognized for 5 minutes.

Mr. MOONEY. Thank you, Mr. Chairman. The Russian invasion of Ukraine has put the work that the Financial Crimes Enforcement Network (FinCEN) does at the forefront of our priorities here in the committee. As Russia's ruble tanked after the sanctions took hold, the incentive for Russian oligarchs to launder their money through the United States grew substantially. We must remain firm in punishing these bad actors and flexible enough to find the strategies that allow them to launder money into the country and our financial system. These goals are critically important to our national security, but we also have an obligation to ensure that the work that FinCEN does and the rules that it creates are not overly-burdensome to small businesses.

Acting Director Das, the Corporate Transparency Act was written to specifically exclude sole proprietors in its definition of a reporting company. However, FinCEN has failed to make that distinction in their reporting company definition. Will FinCEN explicitly exclude sole proprietors from the definition of a, "reporting company?"

Mr. DAS. As the NPRM states, reporting companies that are required to submit beneficial ownership information include corporations and LLCs and other similar entities that are required or that create or form an LLC or a legal entity through the submission of a document to a State secretary of state. That is the scope of the rule. As we have defined it in the NPRM, we requested a number of comments and questions around the scope of the reporting company definition to better understand who or what type of legal entities that definition would capture, and we are taking stock of those comments at this point.

Mr. MOONEY. Okay. In addition to the potential regulatory burdens of some FinCEN rules, I am also concerned about FinCEN's cybersecurity. FinCEN's role in combating illicit finance would make it a target of cyberattacks from Russia and China. Acting Director Das, please talk about what you are doing to ensure that a cyber breach of FinCEN would not jeopardize the information of small business owners.

Mr. DAS. That is an important concern. Again, we have a robust IT framework. And as I mentioned previously, we have what is called a segmented IT architecture, which makes our IT system less vulnerable to hack and intrusion. We conduct regular penetration testing to ensure that any vulnerabilities are exposed and that we prevent any targeted efforts with respect to our IT system. We stay in close communications with Treasury's Office of the Chief Information Officer as well to identify any potential threats to our system. And again, we apply the highest level of security under the FISMA levels of security as well. We work very hard to ensure the integrity of our IT database, and we are taking all of the precautions necessary to do so.

Mr. MOONEY. Thank you. Obviously, it is critical that we get the balance right between keeping illicit financing out of our country and keeping compliance burdens low. Small businesses are the backbone of this economy. We very much need them to succeed in America. In addition to the regulatory burden, we need to ensure that FinCEN can be a good steward of information. The new beneficial ownership database will contain personal information from millions of small business owners. Clearly, if someone were to breach that database, it would be a total disaster.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. HIMES. The gentleman yields back.

The gentlewoman from Pennsylvania, Ms. Dean, is now recognized for 5 minutes.

Ms. DEAN. I thank the Chair, and I thank you, Director Das, for testifying today. I do apologize. I am between two hearings, so I don't want you to think my absence here is due to a lack of interest in your work and what you do. Thanks for being here and for your testimony.

I would like to talk about FinCEN and combating gun violence. I have a bill that was noticed in conjunction with this hearing, the Gun Violence Prevention Through Financial Intelligence Act, which would require FinCEN to collect and analyze bank data to determine what financial indicators might precede a mass shooting, a terrorist attack, or gun violence in our communities, and that the FinCEN would be required to issue an advisory on how banks should use those indicators to comply with their suspicious activity reporting. If insufficient data exists, FinCEN is required to report to Congress within 1 year about why the information they collected was inadequate to publish an advisory.

I don't need to tell you or anybody in this room that gun violence hunts down far too many innocent Americans. Every single year, those numbers are increasing in dramatic fashion. And I saw a tragic statistic earlier this week that guns have become the leading cause of death among children, the leading cause of death in 2020. Our inaction on this issue is, I think, shameful, unforgivable, and really intolerable. We have to have an honest discussion around gun violence.

Director Das, right now, what does FinCEN do? Does FinCEN collect data relative to financial indicators of gun violence? If not, what should we be doing? How can we help financial institutions identify risks of mass shootings, of terrorist attacks, of gun violence? Would you tell us about FinCEN and gun violence?

Mr. DAS. I appreciate that, and the issue of gun violence is very serious, and the impact on children is incredibly important as well. It is tragic. In terms of suspicious activities related to gun violence, again, our reporting regime is one in which financial institutions identify suspicious activities where they know, they have reason to know, or suspect that there is some illicit financial activity that is ongoing, they would report that information. We can work with you in terms of identifying whether or not there may be use in terms of identifying red flags, or typologies, and have a conversation around that. But primarily, at this point, it is what suspicious activity reports are filed by financial institutions around this issue.

Ms. DEAN. And do those reportings include suspicious activity connected to gun violence? Does it specifically lift that up?

Mr. DAS. It could ultimately include that, if that is what a financial institution reports to us. I would have to look—

Ms. DEAN. Would you be able to maybe collect that and—

Mr. DAS. I would have to look closer at this issue to be able to identify whether or not suspicious activity reports specifically raise this issue. So, I would have to get back to you on this.

Ms. DEAN. I would really appreciate that. That will help inform the legislation that I am trying to move forward on. And maybe that is an avenue into combating gun violence that will not be politicized, that will be embraced in a bipartisan way. So, if you could collect that data and share it with us so that we can learn, that would be really terrific.

I think I have a little more time, so I will try one more area of questions. I think you mentioned in your testimony that FinCEN has, "issued two Russia-related alerts to provide financial institutions with more information about typologies and red flags in order to support U.S. Governmental efforts to sanction Russia." You talked about robust engagement with financial institutions. Were your advisories received? In your opinion, how well are financial institutions complying with the sanctions that have been put in place and are continuing to be put in place? What additional resources do you need to ensure full implementation?

Mr. DAS. I appreciate that. I believe the alerts and advisories were well received by financial institutions in terms of providing additional guidance with respect to red flags and typologies. Financial institutions are sensitized to the issue of both sanctions evasion as well as the U.S. financial system being used to hide Russian oligarch assets as well. And my sense is that we are seeing a number of very useful suspicious activity reports coming from U.S. financial institutions with respect to Russian oligarchs, as well as with respect to sanctions evasion.

In terms of resources, again, the most important thing for us is to get FTEs, and then funding to be able to support hiring so that we can do the analytics necessary to evaluate those suspicious activity reports, to evaluate the transactional information that we receive so that we can take that information and translate and provide it to law enforcement as well.

Ms. DEAN. Thank you.

Mr. HIMES. The gentlewoman's time has expired.

The gentleman from Tennessee, Mr. Kustoff, is now recognized for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman. Acting Director Das, I want to thank you for two things, first of all for your service, and second, for agreeing to appear today. We appreciate it.

I kind of thought it was timely that on The Wall Street Journal's website today, there was a story that posted in the headline as, "Russian Sanctions Complicate Paying Ransomware Hackers," and it cites FinCEN. But my question to you is, in terms of reality or practicality, do we have American businesses or companies that have been targeted by ransomware hackers that have to pay ransom to entities that we have sanctioned?

Mr. DAS. There may be situations in which a U.S. business or a company may be subject to a ransomware attack where the ransomware actor is a sanctioned person.

Mr. KUSTOFF. This article again, posted this morning, said that the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and its Financial Crimes Enforcement Network (FinCEN) both have highlighted ransomware payments in recent months. OFAC said in September that it strongly discourages extortion payments and reiterated that it can take action against payers. I guess from a practical standpoint, if a company has been targeted with ransomware, they have to pay a ransom, and the ransom has to be paid to an entity that has been sanctioned by us. What recourse do they have?

Mr. DAS. I appreciate the question. Again, I am here to represent FinCEN and FinCEN's authorities. In terms of the answer to your question, that falls within the scope of OFAC authorities and engagement with the Office of Foreign Assets Control in terms of exactly how its sanctions apply, and what the contours might be, and what flexibility there might be in a particular situation. I am hesitant to go in that direction.

Mr. KUSTOFF. Fair enough. I think you have answered this, but I am going to ask it one more time in a different way. Do you or FinCEN know of American businesses or entities that have been targeted with ransomware by companies or by entities in Russia that have been sanctioned?

Mr. DAS. I am not aware of particular situations in terms of that particular question.

Mr. KUSTOFF. Okay. I am a former United States Attorney. I think I may be the last Presidentially-nominated United States Attorney who has been confirmed by the Senate and the House of Representatives. I am asking this with that in mind, is that, I don't know that FinCEN necessarily has an obligation to the people. I think you do to Congress, to provide evidence of how effectively or efficiently you work. I believe the ranking member asked about how many convictions have been led based on FinCEN's work and actions. I am not going to ask you anything that specific, but if you were talking to any of my constituents, how would you describe the effectiveness or efficiency of FinCEN?

Mr. DAS. First of all, in terms of this hearing, it is clear that we need to do a better job in terms of communicating how effective FinCEN's work is and how effectively we work with law enforcement and with the intelligence community. Again, the work that we do is invaluable in terms of supporting law enforcement, and U.S. Immigration and Customs Enforcement's (ICE's) efforts, and OFAC's efforts to target bad actors that might abuse the U.S. financial system and, for that matter, the international financial system. The information that we use is critical for law enforcement to go after a range of criminal threats, everything from human smuggling, human trafficking, online child sexual exploitation, and money laundering by drug trafficking organizations, across-the-board. All of the types of criminal activity that are identified in our AML/CFT national priorities, the information that we get, it cannot be overstated in terms of how valuable it is for law enforcement to be able to identify, target, and then prosecute individuals.

Mr. KUSTOFF. I appreciate that. Is there anything you think that FinCEN could publish, not for the American people, but for us, to demonstrate again your effectiveness and efficiency?

Mr. DAS. The first step in that, again, is the report required under Section 6201 of the AML Act that DOJ is required to provide in terms of the value of BSA information for DOJ and for law enforcement. I am happy to work with you in terms of other measures or indicia of success as well to be able to make a better case for what we do.

Mr. KUSTOFF. Thank you. We appreciate your service. And I yield back.

Mr. HIMES. The gentleman's time has expired.

The gentleman from New Jersey, Mr. Gottheimer, who is also the Vice Chair of our Subcommittee on National Security, International Development and Monetary Policy, is now recognized for 5 minutes.

Mr. GOTTHEIMER. Thank you, Mr. Chairman, for holding this critical hearing.

As technology advances and terrorists continue to innovate, Federal enforcement efforts must keep pace so that we can crack down on each new method of financing terror, so I appreciate this conversation. Mr. Das, thank you for being here with us today. I am a strong proponent of establishing appropriate guardrails around the cryptocurrency industry to ensure the market matures in the United States. The industry wants clarity and consistency. One of the most critical areas to me is the area of anti-money laundering and counterterrorism financing. What is FinCEN doing to help prevent actors, such as Hezbollah and Russians seeking to evade sanctions, from utilizing cryptocurrency as a finance tool?

Mr. DAS. Again, thank you. FinCEN has been at the forefront in terms of ensuring that cryptocurrency exchanges and cryptocurrency administrators are subject to the same AML/CFT program requirements that MSBs are and other financial institutions are as well. Again, cryptocurrency exchanges, because of their AML program requirements, file suspicious activity reports where there are indicators or they may have a reason to know or suspect that there might be illicit financial activity. And that includes activity by foreign terrorist organizations and other bad actors as well. When we do receive those suspicious activity reports, we work very closely with the intelligence community and with law enforcement.

Mr. GOTTHEIMER. Thank you. Last year, FinCEN released its first national anti-money laundering and counterterrorism financing priorities list, as you know, which included domestic terrorists such as those radicalized online. This week, I am sending a request to the Appropriations Committee to request additional resources for your Agency, particularly related to targeting domestic financing. Could you elaborate on how this funding could be helpful and how FinCEN could use this funding to stop terrorist attacks before they even get beyond the planning phase?

Mr. DAS. I'm sorry. I am not aware of the additional financing with respect to domestic violent extremism and this bill.

Mr. GOTTHEIMER. Are there more resources that you think you could use?

Mr. DAS. Yes. Again, we need additional resources across-the-board with respect to everything that FinCEN does, in terms of its support for law enforcement and for the intelligence community across-the-board with respect to terrorism.

Mr. GOTTHEIMER. In the remaining minutes we have, can you talk a little bit more about the priorities list?

Mr. DAS. Sure. The priorities list was developed over a period of time, 180 days, in terms of significant engagement with the law enforcement community and with respect to regulators and others, in terms of identifying the key priorities that the United States faces in terms of combating criminal activity and other types of illicit activity as well. The intent of the AML/CFT priorities list was to provide financial institutions with an understanding of what law enforcement priorities might be, for them to better hone and direct their AML/CFT programs to identify suspicious activities that might align with the interests of law enforcement and the types of priorities that we have in the United States.

What we have heard from financial institutions is that it has been valuable. To the extent that financial institutions have used those AML/CFT priorities, that has been valuable in terms of them developing their AML/CFT programs and targeting their AML/CFT programs as well. Again, the AML Act provides that we need to issue regulations that direct financial institutions to incorporate those AML/CFT priorities into their AML/CFT programs. We are working on that regulation at this point in terms of what the contours of that might look like.

Mr. GOTTHEIMER. Thank you. I yield back. Thank you, Mr. Chairman.

Mr. HIMES. The gentleman yields back.

The gentleman from Tennessee, Mr. Rose, is now recognized for 5 minutes.

Mr. ROSE. Thank you, Mr. Chairman, and thanks to Ranking Member McHenry. Acting Director Das, thank you for being here and for spending so much time with us today. It is good to see you again, and I appreciate you meeting with me earlier this week. It was great to discuss the issues that have been plaguing independent ATM operators, as you discussed earlier with my colleague, Mr. Luetkemeyer.

As many people know, independent ATM operators across the country have had a tough time finding banks that will provide them with services since Operation Choke Point. Despite officially ending in August of 2017, the operation to de-bank certain industries is still impacting ATM operators today. So, I was thankful to hear your commitment to work with the other agencies to issue a joint statement underscoring that there is no particular risk associated with that category of customers.

Acting Director Das, as I mentioned in our meeting, I am concerned about the current BSA process in which the Federal Government deputizes financial institutions. And I would say maybe at this point, just to broadly state my view, that the cost of this regulatory framework, I think, is troubling, and certainly even the path that we are headed down with respect to beneficial ownership is troubling to me, and the cost to our business community for that regulation is something that is very much in my sights. I spent 10

years on a bank board where I was tasked with looking at suspicious activity reports and the lack of feedback that banks and other financial institutions receive on whether a specific filing was helpful in assisting law enforcement is extremely troubling to me. As I have said, it is like shooting a target in the dark with a blindfold on.

Acting Director Das, would it be possible for your Agency to effectively do its job without the participation of financial institutions?

Mr. DAS. Financial institutions are one of our most important partners being able to make the AML system.

Mr. ROSE. Thank you. And it costs them a lot of money to help you do your job by sending the data that law enforcement then has access to. I think the current system is somewhat broken, where these financial institutions are spending tremendous amounts of time and money on BSA filings, unfortunately, mostly without any feedback. There must be a more efficient process, and I know you have talked today about some of the efforts aimed at hopefully giving them some of that feedback. How much money do you think financial institutions spend every year on BSA filings in the United States?

Mr. DAS. I don't have a particular statistic on that point, but I—

Mr. ROSE. I think we could agree it is a lot, right?

Mr. DAS. Yes.

Mr. ROSE. And certainly, you have talked about the resource constraints that FinCEN faces in terms of fulfilling its mission of dealing with that data that comes to you. Would it be useful to tell financial institutions whether a filing was or was not valuable to law enforcement?

Mr. DAS. Again, the AML Act places a focus in terms of helping financial institutions understand how we are using our suspicious activity reports in relation to providing them to law enforcement and others. We are using a number of the vehicles through the AML Act to engage with financial institutions, including FinCEN Exchanges, Innovation Hours, et cetera, to help them understand better how we are using suspicious activity reports and what is valuable in terms of what they might be providing to us in terms of suspicious activity reports.

Mr. ROSE. In the current system, does law enforcement or another agency user of FinCEN data have to explain on an individual inquiry basis what the data that they are gathering is going to be used for?

Mr. DAS. There is no requirement on law enforcement to provide a specific SAR-by-SAR analysis of how they are using that information.

Mr. ROSE. Do you believe that FinCEN's current authority would enable you to implement some sort of requirement relative to a requirement that the user explain what they are seeking data for each time they access the database?

Mr. DAS. In terms of our engagement with law enforcement and financial institutions, I think that we can work under the existing framework to provide greater transparency in terms of how law enforcement may be using suspicious activity reports. Again, suspicious activity reports are just one piece of what law enforcement

does in terms of an overall investigation. It complements information coming from a number of different sources, through subpoena authority, and through other investigative techniques. So often, drawing a one-to-one line between a suspicious activity report and a particular investigation or prosecution is just challenging.

Mr. ROSE. I understand that. And I guess I will just conclude, if you will indulge me for a second, by saying that I think what I am hearing today from a large number of the Members is that we want to see that kind of quantitative, that kind of actual objective data. And so, with that, I yield back.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Illinois, Mr. Garcia, is now recognized for 5 minutes.

Mr. GARCIA OF ILLINOIS. Thank you, Mr. Chairman, and, of course, thank you, Acting Director Das for your testimony today. At its best, FinCEN has the potential to set a strong anti-corruption agenda, disrupting the shadowy world of shell companies, oligarchs, and arms traffickers whose financial crimes have harmful consequences for everyday people. In order to fulfill that potential, the anti-corruption agenda requires our support and careful oversight to ensure transparency and progress, and I look forward to your partnership on these issues. With that in mind, I would like to move on to my first question.

The Corporate Transparency Act is the most important change to U.S. anti-money laundering law in decades, and FinCEN's proposed implementation rule is a strong step in that direction. However, as my colleagues have noted, several phases of rulemaking are left. Final rules have been overdue since January 1st of this year. Will FinCEN commit to issuing final rules by the International Anti-Corruption Conference, which the U.S. Government will be hosting in December of this year in Washington, D.C.?

Mr. DAS. Thank you for that question, Congressman. We are committed to completing the second notice of proposed rulemaking and the suite of Corporate Transparency Act rules by the end of the year, so we will be issuing a notice of proposed rulemaking with respect to the access rule. I can't commit on a particular timeline with respect to the additional rules. We are doing a lot of work and we are working as hard as we can in terms of getting those rules done.

Mr. GARCIA OF ILLINOIS. Thank you. President Biden's strategic plan for countering corruption acknowledges the importance of a transparent and accessible beneficial ownership registry to effectively combat terrorist financing, corruption, and other crimes. Similar registries in the U.K. and the EU have public accessibility requirements. They also have examples of accountability groups, journalists, and members of the public successfully identifying financial crimes from the available data, but under the Corporate Transparency Act, information from the registry can only be shared for law enforcement purposes. As FinCEN works to implement this and future projects, do you believe that public-facing databases could be more effective than private databases, and how can FinCEN harness the power of civil society in the anti-corruption work that it does?

Mr. DAS. Thank you for that question. Again, we are focused on implementing the Corporate Transparency Act (CTA). The Corporate Transparency Act has very specific rules with respect to access by law enforcement, by regulators, and by other government agencies, as well as State and local law enforcement. It is perceptive in this regard, and again, we are focused on implementing the CTA at this point. Again, civil society plays an important role in anti-corruption efforts. And from our perspective, we look forward to engaging with civil society in terms of their feedback and perspectives, either through the notice-and-comment process or otherwise, in terms of the effectiveness of the database, the contours of the database, and then the construction of the database as well.

Mr. GARCIA OF ILLINOIS. Thank you for that. My final question is on real estate. Home ownership has historically been a way to build modest wealth for otherwise marginalized communities, but as you know, real estate is one of global kleptocrats' most important assets, as my constituents are feeling the effects. While real estate investors take cash offers from foreign kleptocrats, working-class families are priced out from home ownership in their neighborhoods. This problem is particularly acute in Latino and Black communities, and the community that I represent, for example, was harmed during the Great Recession. I was encouraged to see FinCEN beginning to work on regulatory rules in the real estate sector. Director Das, will you commit to having a rule published by the International Anti-Corruption Conference this December?

Mr. DAS. We issued an NPRM last December, and we received a number of comments at the close of the notice-and-comment period, which was in mid-February. We are reviewing those comments and considering next steps in terms of a potential proposed rule. We are working incredibly hard on this, as we also work on the beneficial ownership database, as well as the other AML Act deliverables, so that makes it difficult for me to commit to a precise timeline.

Mr. GARCIA OF ILLINOIS. Thank you, Mr. Das.

Mr. Chairman, I yield back.

Mr. HIMES. The gentleman's time has expired.

The gentleman from Ohio, Mr. Gonzalez, is now recognized for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman, and thank you, Acting Director Das, for your testimony today. I want to pick up on the online child sexual exploitation conversation. I just want to understand the organization's priorities and how you are effectively combating it. As an organization—and you can give me ballpark—what percent of your budget is targeting crackdowns on online child sexual exploitation?

Mr. DAS. In terms of the overall budget, it is difficult for me to provide a ballpark.

Mr. GONZALEZ OF OHIO. Ballpark is fine.

Mr. DAS. But I can tell you that we have one staffer who is dedicated to the issue.

Mr. GONZALEZ OF OHIO. One staffer?

Mr. DAS. One staffer in—

Mr. GONZALEZ OF OHIO. One individual staffer?

Mr. DAS. One individual staffer.

Mr. GONZALEZ OF OHIO. Does that staffer have a—

Mr. DAS. It is dedicated. But in addition, a number of other staffers and a number of other personnel support the effort more generally, but we have somebody who is dedicated to the effort full time across human trafficking, human smuggling, as well as online child sexual exploitation.

Mr. GONZALEZ OF OHIO. So, one staffer. How does that compare to other priorities like—the top priority and how many staffers are leading that effort, and compare that to money laundering.

Mr. DAS. This is one full-time staffer. We have folks focused on a number of different fronts across the whole suite of issues around ensuring that we have effective AML/CFT programs in place. Financial institutions are providing suspicious activity reports, not only on the many priorities in the national AML/CFT priorities but as well as particularly on human smuggling, human trafficking, and online child sexual exploitation. That individual staffer is focused on reviewing suspicious activity reports that are filed, and then working very closely with IRS Criminal Investigation (IRSCI), which is very focused on this issue, as well as the Joint Criminal Opioid and Darknet Enforcement Network (JCODE), which is also very focused on this issue as well. So, it is a focal point in terms of collecting the information, looking at the information, and then providing that, and working with law enforcement so that they can use that information to investigate these acts.

Mr. GONZALEZ OF OHIO. Okay. And then, how closely does FinCEN work with private industry to share information and best practices to identify and stop payment methods for the purposes of online child sexual exploitation?

Mr. DAS. I apologize, Congressman. If you could repeat that question. I didn't—

Mr. GONZALEZ OF OHIO. Sorry. How closely does FinCEN work with private industry to combat online child sexual exploitation?

Mr. DAS. Again—

Mr. GONZALEZ OF OHIO. On the payment side specifically.

Mr. DAS. We work with financial institutions in terms of suspicious activity reports, and enhancing awareness with respect to this issue. We have issued a couple of different advisories and notices on online child sexual exploitation in child sexual abuse material as well. In 2020, we issued an advisory around this issue. Specifically, it was a supplemental advisory. And in September of 2021, we issued a notice that identified this as a particular issue of focus for financial institutions, especially against the backdrop of the pandemic. We identified a particular code around online child sexual exploitation in the event that financial institutions were providing a SAR on this specific issue, that it would be identified with a particular marker that we would easily be able to track.

And that notice actually was incredibly effective. We received over 1,600 suspicious activity reports from the period of September 2021 through December of 2021, and this year through April, I believe mid-April, we have received about 650 suspicious activity reports on this issue as well. Again, we are attuned to this issue, we are very focused on it, and we are doing what we can.

Mr. GONZALEZ OF OHIO. Can I ask a quick question? Do you think one staffer is enough, and it may be that you don't have the

budget, I get that, but do you think the one staffer has the bandwidth to effectively monitor all of the SARs related to child sexual exploitation?

Mr. DAS. Again, this is a difficult issue. We should be providing resources across our entire envelope. Again, we are meeting incredibly difficult resource constraints against all of the types of activities that we do.

Mr. GONZALEZ OF OHIO. Okay. Just a general observation, and then I will yield my time back. It gives me pause to know that there is only one staffer. And I know that you are budget-constrained, but it is an enormous issue and there is nobody more vulnerable than a child who is being sexually abused, whether it is online, in a home, whatever it is. We know from our office's work with the FBI, the local FBI office in Cleveland, that the pandemic had a particularly nasty effect on the increases in child sexual exploitation. My ask would be that your office is willing to work with us on ways to get you, whether it is more funding, more tools, more resources, whatever it is, but this needs to be a bigger focus than just one staffer.

And with that, I yield back.

Mr. DAS. And we would like to dedicate more resources, and we will take you up on that offer to work with you.

Mr. HIMES. The gentleman's time has expired.

The gentleman from South Carolina, Mr. Timmons, is now recognized for 5 minutes.

Mr. TIMMONS. Thank you, Mr. Chairman, and thank you, Acting Director, for being with us today. I want to talk about implementation of the Corporate Transparency Act, which is a pretty deceptive name, in my opinion, for the bill, as its scope goes far beyond large corporations. Before I came to Congress, I started a number of small businesses. It was hard work, and, honestly, probably the hardest work was dealing with the onerous government regulations at the Federal, the State, and the local level. Way too much of my time was spent trying to please bureaucrats rather than trying to please my customers. I don't think it should be that way.

So, a part of my concern with the CTA was the additional compliance burden it places on businesses. The large corporations will be fine. They have armies of lawyers, accountants, and compliance departments. They can handle everything, but for small business owners, it is a big headache. I was my own compliance department. And by the way, I would venture to guess that out of the tens of millions of covered entities of this law, the vast majority have no idea what FinCEN even is. There is a big education piece to this, and a somewhat large potential for bad actors to take advantage of the beneficial ownership requirements to scam these folks and steal their identities. Do you share these concerns? Are you striving to implement these new rules in the least intrusive way possible on small businesses?

Mr. DAS. That is what the AML Act and the CTA directs us to do, is to do it in a way that minimizes the burden on small businesses. Again, we are focused on developing a database that is effective, and that minimizes the burdens on small businesses while ensuring that we have a database that is effective and provides

highly-useful information to law enforcement. That is our prime directive with respect to the database.

In terms of the reliability of the database, I think again, we are very focused on ensuring the integrity of the database and ensuring that it meets the highest standards of IT protection from hacks and otherwise. We are very focused on privacy interests and considerations around those issues in the context of the CTA. And the notice-and-comment process has provided us with a significant amount of feedback and useful feedback in terms of thinking through how the rules work, and how they could be improved, and we will be working on that in the coming months.

Mr. TIMMONS. How do you feel that it is going so far?

Mr. DAS. We are working incredibly hard on this effort. It is difficult in a resource-constrained environment, but we are making a lot of progress. The team is incredibly dedicated. They are tired, I can tell you that. But we are making progress both in terms of the reporting rule, the access rule, and the overall database work. It is an incredibly complicated effort. We have to get it done right. And we are spending time and effort in making sure that the rules work together, the database is built appropriately, and is one that can be used effectively by law enforcement and other stakeholders.

And I agree with your point that it is incredibly important for companies and individuals that have to report information to understand what the rules are, and it is very important for us. And we are very focused on it from a FinCEN perspective to develop an outreach strategy in an effort to engage with stakeholders, with industry groups, with businesses, and with State secretaries of states so that they understand what the contours of the rules are, and they understand what the obligations are in a way that ensures that they can do so in the least burdensome manner as well.

Mr. TIMMONS. Sure. Thank you. This is going to be a huge amount of valuable, highly-sensitive data. What is your cybersecurity plan to make sure that it stays where it is supposed to be?

Mr. DAS. Again, we are very focused on cybersecurity. We plan on applying high standards, the highest standards with respect to cybersecurity for the beneficial ownership database. With respect to our existing system of records, our database, we apply FISMA high standards with respect to the database. We do regular penetration testing. We engage closely with the government security accountability committee which governs security around IT databases as well. And we plan on doing this with respect to the beneficial ownership database, because we recognize that that database holds very sensitive information.

Mr. TIMMONS. Thank you. The government has had a lot of breaches recently, and I would hate to have this be another one. So, I appreciate you prioritizing that.

Thank you, Mr. Chairman. I yield back.

Mr. HIMES. The gentleman yields back.

The gentleman from Wisconsin, Mr. Steil, is now recognized for 5 minutes.

Mr. STEIL. Thank you very much, Mr. Chairman. And thank you for being here, Mr. Das. I really appreciate it.

It has been discussed a little bit, but I want to dive in a little further on BSA data, SARs, the volume, who is looking at it, and

the effectiveness of this. BSA data is meant to be highly useful for law enforcement. To what extent is law enforcement providing feedback to those who file BSA data? I am looking for that feedback loop.

Mr. DAS. We regularly engage with law enforcement in terms of the suspicious activity reports. We have a number of liaisons from law enforcement who sit within FinCEN and that we work closely with in terms of the use of SARs, priorities that law enforcement has, as well as feedback that we get. When we work with law enforcement and provide them with reports, we often communicate with them on the value of the suspicious activity reports that we have or other information that we give to law enforcement, and we, across-the-board, get positive feedback from law enforcement.

Mr. STEIL. That is good. Let me just scale this, because I think it is important. In March of this year, 325,378 SARs were filed by financial institutions. What percentage of those might receive feedback in a given month?

Mr. DAS. Again, we do not collect SAR-by-SAR feedback. There are a number of challenges in doing so.

Mr. STEIL. Understood. Rough math, just to scale it, because I think it is relevant on this feedback loop because I will tell you, on my side, many people feel that the SARs information is just going into a black hole. My concern is that people are filing what I call defensive SARs. They are filing SARs to be protective of themselves so they don't have an investigation coming upon them rather than doing what we are really trying to do, which is to identify suspicious activity which is actually helpful in your operations. Not that you aren't providing feedback to some and, in particular, cases where that information is useful. But I think many people feel that there is a giant black hole, and my concern is then that perception can become reality for many of these banks who then engage in filing what I view as defensive SARs, which doesn't really help us. Finding the needle in a haystack is dependent on a handful of things, one of them being how big the haystack is.

And so, if we can find a way to bring this haystack down, I think we may actually find ourselves in a position to more easily find the needle, if you will. And I think that is one of the things that this committee should spend time on, in particular on the regulatory side. And on the legal side of how we set the thresholds to file these SARs, I think it would be quite beneficial to remove some of the noise that is in these documentations.

Let me shift gears, because we have hit that a couple of times today. One of the things I just want to touch base with you on is there has been a lot of concern among some of my colleagues, and some of the media, talking about the use of digital assets to avoid U.S. sanctions. I think some of it is unfounded and misplaced, especially given some of the level of visibility we have in open ledgers maintained on blockchain. A counselor to the Deputy Treasury Secretary recently commented that crypto wasn't a major concern, given the huge scale of what bad actors would have to move. Do you agree that digital assets aren't a major sanctions-evasion mechanism?

Mr. DAS. Again, in our sanctions evasion alert, we have alerted financial institutions to the potential for cryptocurrency being used

as a channel for sanctions evasion. We have not seen significant activity, large-scale activity, in terms of the use of cryptocurrency for sanctions evasion. But again, there is potential for cryptocurrency to be used for sanctions evasion, and we are ensuring that financial institutions are alert to this issue, and if there is such sanctions evasion, to submit a suspicious activity report highlighting it.

Mr. STEIL. I appreciate your feedback on this. In the very limited time we have left, one of the things I have been very concerned about is fentanyl coming into our communities. It is the number-one cause of death among individuals aged 18 to 45. You are not involved in securing our borders. I am going to park that for a moment. But I am curious as to what FinCEN is doing to stop illicit fentanyl traffickers from laundering their profits through our financial system.

Mr. DAS. We receive suspicious activity reports with respect to drug trafficking, narco trafficking, fentanyl as well. We work very closely with law enforcement in terms of our efforts to help them understand money laundering organizations that are related to drug trafficking organizations. We work closely with HSI, with the FBI, and with DEA, and we have a close partnership with them in terms of helping them understand the information that we have and helping them analyze the information that we have to be able to better target this issue.

Mr. STEIL. Thank you very much. Thank you for being here. Mr. Chairman, I yield back.

Mr. HIMES. The gentleman's time has expired.

I would like to thank Acting Director Das for his testimony today.

The Chair notes that some Members may have additional questions for this witness, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to this witness and to place his responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

The hearing is now adjourned.

Mr. DAS. Thank you.

[Whereupon, at 12:50 p.m., the hearing was adjourned.]

A P P E N D I X

April 28, 2022

Statement by

Himamauli Das

Acting Director

Financial Crimes Enforcement Network

United States Department of the Treasury

before the

Committee on Financial Services

U.S. House of Representatives

April 28, 2022

Good morning. My name is Him Das, and I am the Acting Director of the Financial Crimes Enforcement Network (FinCEN). Chairwoman Waters, Ranking Member McHenry, and distinguished Members of the Committee. Thank you for the invitation to appear before you today to provide an update on FinCEN's implementation of the Anti-Money Laundering Act of 2020 (AML Act), including the Corporate Transparency Act (CTA). This morning, I hope to demonstrate the value FinCEN adds to the nation's regulatory, law enforcement, and national security infrastructure, and the critical role it has played, and continues to play, in transforming our nation's anti-money laundering (AML) regime from post-9/11 to post-pandemic; from al-Qaida to artificial intelligence and digital assets.

Until recently, the overarching legal foundation of the U.S. anti-money laundering/combating the financing of terrorism (AML/CFT) regime reflected the post-9/11 moment. Just as earlier iterations of the Bank Secrecy Act (BSA) were focused on countering the dominant policy concerns of their times—such as combating drug-related financial flows—the updates made to the BSA by the USA PATRIOT Act after 9/11 emphasized disrupting the money flows of terrorist organizations such as al-Qaida through the traditional banking system.

The AML Act has helped put FinCEN in the position to address today's challenges, such as illicit use of digital assets, corruption, and kleptocrats hiding their ill-gotten gains in the U.S. financial system, including through American shell companies and real estate. It also highlights FinCEN's unique tools and expertise to combat both longstanding threats, as well as new ones, such as ransomware and other cyber-enabled threats and the use of the dark web to engage in illicit activity, such as the online exploitation of children.

The AML Act also provides tools to approach innovations in a way that recognizes not only the opportunities they present, but the risks that they pose. One of the purposes of the AML Act is to encourage technological innovation and the adoption of new technology by financial institutions to make the AML/CFT framework more effective. And, it directs FinCEN to "streamline, modernize, and update the AML/CFT regime of the United States." It also placed by statute national security front and center in FinCEN's mandate.

Current events often make clear the importance of an AML/CFT framework that is well designed and effective in preventing bad actors from exploiting the financial system. As the pandemic began to unfold in 2020, FinCEN pivoted its efforts to focus on the effects COVID-19 was having on a range of illicit finance threats around the world. FinCEN issued guidance, advisories, and information about trends and red flags to provide feedback to financial institutions on COVID-19 medical fraud, imposter scams, cyber-enabled crime, and the defrauding of the unemployment insurance system. FinCEN also assisted law enforcement and financial institutions in the recovery of funds stolen via fraud and other COVID-19 related crimes.

In 2021, FinCEN placed a spotlight on ransomware—a scourge that continues to affect schools, hospitals, the U.S. energy grid and oil supplies, and large and small companies around the United States. In October 2021, FinCEN published its first Financial Trends Analysis (FTA) as required

by section 6206 of the AML Act. This report shared with the public ransomware trends and typologies gleaned from financial intelligence provided to FinCEN by financial institutions.[1] FinCEN also published an advisory and hosted a FinCEN Exchange, as required by section 6103 of the AML Act, on ransomware to alert financial institutions to red flags associated with the crime. FinCEN continues to work closely with law enforcement and develops investigative tips and leads based on suspicious activity reporting and blockchain analysis.

Now, the ongoing situation in Ukraine places a renewed spotlight on the importance of an effective AML/CFT regime in providing key insights and information to law enforcement and national security agencies.

Ongoing Situation in Russia/Ukraine

Since the further invasion of Ukraine began, the United States and our international partners have imposed unprecedented financial pressure on the Russian Federation and its leadership. FinCEN is bringing all BSA authorities to bear in support of U.S. government efforts and multilateral efforts. FinCEN has issued two Russia-related alerts to provide financial institutions with information about typologies and red flags. The first alert focused on sanctions evasion,[2] and the second highlighted channels through which oligarchs hide and launder corrupt proceeds.[3] These channels include shell companies, real estate, and the purchase of luxury goods and high-end art.

Additionally, FinCEN is continuing robust engagement with financial institutions through its public-private partnership FinCEN Exchange program, to explore typologies and share best practices. These exchanges enable the private sector to better identify corrupt proceeds of elites, oligarchs, and their proxies, and provide FinCEN and law enforcement with critical information to track, freeze, and seize their assets. We are sifting through suspicious activity and other reports filed by financial institutions to trace beneficial owners of shell companies established by oligarchs, locate hidden assets, and uncover efforts to evade sanctions.

Finally, on March 16, 2022, FinCEN led the effort by the financial intelligence units (FIUs) of Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the United Kingdom, and the United States in issuing a statement of intent to form an FIU Working Group on Russia-Related Illicit Finance and Sanctions.[4] The FIUs affirmed the need to identify

---

[1] *See* FinCEN, "FinCEN Issues Report on Ransomware Trends in Bank Secrecy Act Data," https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data

[2] *See* FinCEN, "FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts," (March 7, 2022), https://www.fincen.gov/index.php/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions

[3] *See* FinCEN, "Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members," (March 16, 2022), https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Elites%20High%20Value%20Assets_508%20FINAL.pdf

[4] *See* Financial Intelligence Units of Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the United Kingdom, and the United States, "Russia-Related Illicit Finance and Sanctions FIU Working

concrete actions that Working Group members can take to enhance financial intelligence on sanctions-related matters; expedite and increase sharing of financial intelligence in sanctions-related matters; discuss FIU best practices, and lessons learned, and identify opportunities for actions and partnerships to combat the threat caused by Russia's unprovoked invasion of Ukraine. The Working Group will also strengthen and facilitate working relationships among FIUs, appropriate public authorities and the private sector addressing that threat, including by engaging with the international Russian Elites, Proxies, and Oligarchs Task Force.

Targeting Corruption

The ongoing tragic events in Ukraine underscore the urgent need to provide transparency to combat corruption. The Biden Administration is aggressively targeting corruption, and recently identified corruption as a core U.S. national security interest. Central to the effort to combat corruption globally is targeting corrupt actors who rely on vulnerabilities in the United States and international financial systems to obscure ownership of assets and launder the proceeds of their illicit activities.

In support of the first-ever U.S. Strategy on Countering Corruption and the Administration's commitment to supporting and bolstering democracy, FinCEN is taking several actions to fight corruption and prevent it from undermining democratic institutions. These actions include implementing beneficial ownership requirements, better addressing money laundering risks in the real estate market, and identifying ways to enhance transparency for investment advisers.

One of Treasury's most significant contributions to the fight against corruption is through the implementation of the CTA, which will establish a beneficial ownership reporting regime to assist law enforcement in unmasking shell companies used to hide illicit activities. Access to beneficial ownership information reported under the CTA would significantly enhance the U.S. government's and law enforcement's ability to protect the U.S. financial system from illicit use. It would also impede malign actors from abusing legal entities to conceal proceeds from criminal acts that undermine U.S. national security, such as corruption, human smuggling, drug and arms trafficking, and terrorist financing. For example, beneficial ownership information can add valuable context to financial analysis in support of law enforcement and tax investigations. It can also provide essential information to the intelligence and national security professionals who work to prevent terrorists, proliferators, and those who seek to undermine our democratic institutions or threaten other core U.S. interests from raising, hiding, or moving money in the United States through anonymous shell companies.

Until the enactment of the CTA in 2021, Treasury had limited ability to identify and collect information about the beneficial owners of certain companies formed in the United States. The CTA requires specified legal entities to submit beneficial ownership information to FinCEN, and for FinCEN to provide timely access to this information to law enforcement, financial institutions, and other authorized users, under specific conditions, to help combat corruption,

---

Group Statement of Intent," (March 16, 2022), https://www.fincen.gov/news/news-releases/russia-related-illicit-finance-and-sanctions-fiu-working-group-statement-intent

money laundering, terrorist financing, tax fraud, and other illicit activity, and to help protect national security. This information must be accurate, complete, and highly useful to authorized government users while minimizing burdens on reporting companies.

In December 2021, FinCEN published in the Federal Register a Notice of Proposed Rulemaking (the "Reporting Rule NPRM") that proposed regulations to implement the beneficial ownership reporting requirements of the CTA, and in particular, defined core terms that will affect the scope of the regulations. This is the first of three proposed regulations that will fully implement the statutory requirements of the CTA. FinCEN received over 240 comments on this first proposal. Commenters weighed in on the breadth of issues considered in the context of the NPRM both in support of and to express concerns with aspects of the Reporting Rule NPRM. The timing of the final rule is not clear yet. It is a complex rulemaking that we need to get right—both for law enforcement and because of the effect that it will have on stakeholders such as small businesses and financial institutions.

FinCEN is currently developing a second NPRM that will propose regulations governing access to beneficial ownership information by law enforcement, national security agencies, financial institutions, and others specified in the statute (the "Access Rule NPRM"). We intend to publish this proposed rule this year.

The final rulemaking to implement the CTA is the revision to the Customer Due Diligence (CDD) regulation for financial institutions, which must be issued no later than one year after the effective date of the final reporting rule. The CTA directs that the revisions should bring the CDD regulation into conformance with the beneficial ownership rules under the CTA and reduce unnecessary or duplicative requirements, among other things. We are considering all options as we develop the Access Rule NPRM, and look forward to receiving public comments on our proposal when it is issued.

In concert with the rulemaking effort, FinCEN is developing the backbone of the beneficial ownership database—the Beneficial Ownership Secure System (BOSS). FinCEN has gathered initial requirements and is completing system engineering, architecture, and program planning, and the initial build of the cloud infrastructure and development environments are in progress. Data security is of the utmost importance, which is why the BOSS is being implemented to meet the highest Federal Information Security Modernization Act (FISMA) level (FISMA High) to secure the beneficial ownership information. The ability to search and access beneficial ownership information will be controlled and tailored by the users' purpose and role. All users will use strong authentication methods to access the information.

The goal of the CTA—and the proposed regulations to implement the CTA—is to combat the proliferation of anonymous shell companies that facilitate the flow and sheltering of illicit money in the United States. These beneficial ownership reporting obligations will make our economy—and the global economy—stronger and safer from criminals and national security threats.

To further implement the President's anti-corruption strategy, addressing the gaps in our anti-money laundering framework that allow the exploitation of the U.S. real estate market is another key area of focus. On December 6, 2021, FinCEN announced the issuance of an Advance Notice of Proposed Rulemaking (ANPRM) to solicit comments from the public to assist in crafting a rule to address money-laundering vulnerabilities in the real estate market. This ANPRM represented the next step in FinCEN's long-running fight to protect the real estate market from exploitation by criminals and corrupt officials. As highlighted in the ANPRM, the current Real Estate Geographic Targeting Order (GTO) program requires title insurance companies to file reports concerning non-financed purchases above $300,000 of residential real estate by certain legal entities in 14 metropolitan areas of the United States.

FinCEN issued these GTOs to ensure that law enforcement and national security agencies have relevant information concerning the approximately 25 percent of residential real estate transactions that proceed without financing from a bank or similar financial institution with full AML/CFT program requirements. FinCEN first issued the real estate GTOs in January 2016 and our law enforcement partners have consistently assessed that the GTOs produce valuable information that helps them target illicit activity. Against the backdrop of requests from law enforcement, FinCEN has renewed the GTOs, and when doing so has periodically expanded the covered geographic areas and lowered the reporting price threshold, based on feedback from law enforcement, as well as our own analysis.

FinCEN is carefully studying the 150 comments we received in response to the real estate ANPRM. These comments will help us move toward the next step, a proposed rule to address the illicit finance threats to the real estate market. While it is still too early to identify the scope of any NPRM or final rule, we are working to ensure that the requirements would be carefully crafted to result in valuable information for law enforcement, regulators, and the intelligence community, as well as to help the real estate sector protect itself from abuse by corrupt and other bad actors.

FinCEN continues to assess the illicit finance risks related to non-bank types of financial institutions that are not subject to comprehensive AML/CFT requirements to determine whether additional AML/CFT measures would be appropriate. As highlighted in the 2022 National Money Laundering Risk Assessment, the lack of a comprehensive AML/CFT regulatory framework for investment advisers may create vulnerabilities that illicit actors may be able to exploit.[5] In 2015, FinCEN issued a NPRM on investment advisers, but did not issue a final rule.

FinCEN, in coordination with the Treasury's Office of Terrorist Financing and Financial Crimes, is engaged in several lines of effort to better understand the nature of any AML/CFT risks presented by investment advisers and the specific channels through which those risks are transmitted. FinCEN's ongoing efforts include engaging with law enforcement, the Securities and Exchange Commission, and the Financial Industry Regulatory Authority. We are also

[5] See Treasury, "National Money Laundering Risk Assessment," (February 2022), https://home.treasury.gov/news/press-releases/jy0619

exploring how to use FinCEN's information collection authorities to enhance transparency in this sector, including regarding how Russian elites, proxies, and oligarchs may use hedge funds, private equity firms, and investment advisers to hide their assets.

This work is critical to scoping a potential rule to address the AML/CFT risks associated with investment adviser activity and to avoid duplicating regulatory efforts or placing undue burdens on small businesses. Even though investment advisers in the United States are not expressly subject to AML/CFT requirements under BSA regulations, investment advisers may fulfill some AML/CFT obligations in certain circumstances. For example, investment advisers may perform certain AML/CFT functions because they are part of a bank holding company, are affiliated with a dually-registered broker-dealer, or share joint customers with a BSA-regulated entity such as a mutual fund.

Further, as with any regulatory framework, it is important that sufficient resources are dedicated to outreach and engagement with newly covered financial institutions, coupled with effective examination and enforcement, in order to foster compliance. FinCEN will need to further consider the resource implications of a possible rule imposing AML/CFT obligations on investment advisers that could result in substantial additional supervisory and examination responsibilities.[6]

Effective Anti-Money Laundering Programs

We must ensure that the AML/CFT regime reflects modern national security needs, attacking threats as they exist in 2022 and as they continue to evolve. Effective AML/CFT programs are an invaluable tool in preventing current threats such as ransomware, stopping Paycheck Protection Program fraud, and rooting out corrupt Russian oligarchs, among other financial crimes. The AML Act imposes more than 40 requirements on FinCEN that are designed to make the AML/CFT framework more effective. It also recognizes that an effective and reasonably designed AML/CFT program is the cornerstone of a financial institution's ability to support law enforcement efforts to combat illicit finance. To support efforts by financial institutions to better understand U.S government priorities, and to incorporate those priorities into their AML/CFT programs, FinCEN published the first government-wide list of national AML/CFT priorities in June 2021.[7] The AML/CFT priorities confirm a broad range of threats to the integrity of the U.S. financial system and our national security, in addition to the financing of terrorism. We will update these priorities regularly, and that will help us keep pace with the shifting threat landscape.

---

[6] *See* North American Securities Administrators Association (NASAA) "2021 Investment Adviser Section Annual Report," (April 2021) at p. 1. *See also* Investment Adviser Association Report, "Investment Adviser Industry Snapshot 2021: Revolution Imagined," (July 2021, Second Edition) at p. 3, and SEC's Information About Registered Investment Advisers and Exempt Reporting Advisers.

[7] *See* FinCEN "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

The AML Act describes certain factors that FinCEN is required to take into account as we consider minimum standards for AML/CFT programs and work toward new regulations that would require financial institutions to incorporate the national AML/CFT priorities. These include the private and public costs and benefits of AML/CFT programs, the need to extend financial services to the underbanked while preventing criminal abuse, the role of "effective" AML/CFT programs in protecting national security and preventing illicit finance, and that AML/CFT compliance programs should be "risk-based" and "reasonably designed to assure and monitor compliance."

The AML Act further incentivizes feedback loops among financial institutions, regulators, and law enforcement in other ways. It emphasizes and codifies public-private information sharing, in which FinCEN engages through FinCEN Exchanges and Innovation Hours. We have held FinCEN Exchanges to share information among FinCEN, law enforcement, and financial institutions on ransomware,[8] on suspicious activity report (SAR) reporting with a regional focus,[9] and on environmental crimes.[10] These have been productive exchanges, and we will be holding more. Typically, a FinCEN Exchange session includes participants from law enforcement, financial institutions and, as appropriate, other private sector entities, for the purpose of sharing information regarding typologies, threats, and vulnerabilities. This increases visibility and transparency for participants, and also informs internal BSA compliance and risk management processes. It also strengthens the financial intelligence received back from stakeholders through suspicious activity reporting, which in turn assists law enforcement and enhances FinCEN's development of analytical products such as advisories and public notices.

Another key feedback loop in the AML Act is the requirement that FinCEN at least twice a year publish threat pattern and trend information derived from suspicious activity reports to provide feedback to financial institutions regarding the use and value of these reports. In accordance with Section 6206, FinCEN published two of these FTA reports last year. As previously mentioned, the first FTA focused on ransomware. In December 2021, FinCEN published the second FTA focused on environmental crimes. FinCEN will publish additional FTA reports this year as required by the AML Act, and we expect that at least one of them will again focus on ransomware.

We continue to engage actively in the Bank Secrecy Act Advisory Group (BSAAG), which allows financial institutions, regulators, and law enforcement to engage directly to find ways to improve the AML/CFT framework. In May 2021, FinCEN launched the BSAAG Innovation and Technology Subcommittee, as required by Section 6207 of the AML Act, and the BSAAG Information Security and Confidentiality Subcommittee, as required by Section 6302. We have

[8] *See* FinCEN, "FinCEN Holds Second Virtual FinCEN Exchange on Ransomware," (August 10, 2021), https://www.fincen.gov/news/news-releases/fincen-holds-second-virtual-fincen-exchange-ransomware

[9] *See* FinCEN, "FinCEN Exchange Brings Together Public and Private Stakeholders to Discuss Bank Secrecy Act Suspicious Activity Reporting Statistics," (November 9, 2021), https://www.fincen.gov/news/news-releases/fincen-exchange-brings-together-public-and-private-stakeholders-discuss-bank-0

[10] *See* FinCEN, "FinCEN Holds FinCEN Exchange on Environmental Crimes and Related Financial Activity," (November 16, 2021), https://www.fincen.gov/news/news-releases/fincen-holds-fincen-exchange-environmental-crimes-and-related-financial-activity

a wide range of participants in these two new Subcommittees including representatives from the federal functional regulators, state banking supervisors, law enforcement agencies, and a variety of financial industry participants, such as depository institutions, casinos, money services business, securities, FinTechs, and digital asset service providers.

These two new Subcommittees are tackling important issues. The Innovation and Technology Subcommittee is focused on innovation themes related to digital identity, the coverage of payment processors under current regulations, and banking relationships with FinTech entities. The Information Security and Confidentiality Subcommittee priorities are looking at third-party vendor relationships and current information security technologies. We are working with the Subcommittees so that they can advise the BSAAG plenary in ways that can help shape our thinking on these important areas.

Another enhancement to FinCEN's feedback mechanism was the establishment of Domestic and Foreign FIU Liaisons in the AML Act to expand engagement with financial institutions and foreign partners. FinCEN has not had the resources to create either the Office of Domestic Liaison—to be led by a Senior Executive Service official overseeing at least six geographically dispersed senior FinCEN employees—or to hire at least six Foreign FIU Liaisons, as required by Sections 6107 and 6108 of the AML Act, respectively. We have requested FY23 appropriations to realize the legislative vision embodied in these two provisions.

Domestic Liaisons would allow FinCEN to improve significantly on the FinCEN-to-financial-institution segment of the feedback loops envisioned by Congress. These Domestic Liaisons will be located in financial centers around the country and will engage directly with regional financial institutions to not only provide those institutions with insights on what's effective in their reporting, but also to hear input and provide feedback on an ongoing basis about how FinCEN can execute its mission even more effectively.

Foreign FIU Liaisons will play a critical role in enhancing international information sharing and the efficiency of international cooperation to combat money laundering. We have seen that the presence of foreign liaisons can create incredible opportunities. FinCEN's one overseas liaison today is at Europol, and that liaison has played a crucial role leveraging existing relationships to organize the FIU Working Group supporting our efforts to enhance information sharing to respond to the threats posed by Russia's invasion of Ukraine. We look forward to achieving similar objectives in key jurisdictions globally.

The AML Act also requires annual training for bank examiners to enable them to better understand risk profiles and warning signs that an examiner may encounter during examinations. The training requirement reflects concerns that financial institutions have long expressed about how examiners evaluate AML/CFT programs and the degree to which those programs are effective and guard against money laundering. Options are largely dependent on funding: considerations include the need for human capital for ongoing design, updating, monitoring, and delivery of the annual training program, as well as technology for delivery and tracking.

The AML Act also places the modernization of the AML/CFT framework—and the role of innovation in that modernization effort—front and center. As required by the legislation, we are working to find ways not only to revise or eliminate regulations that are "outdated" or "redundant," but also to identify ways to provide opportunities for financial institutions to adopt innovative technologies that help them enhance their compliance programs.

Last December, we issued a Request for Information (RFI) pursuant to section 6216 of the AML Act.[11] That RFI sought public input on ways in which FinCEN can streamline, modernize, and update the AML/CFT framework so that it can continue to protect U.S. national security and prevent illicit finance in a way that promotes an efficient allocation of resources.

We received 140 comments, and are carefully reviewing every comment with the goal of developing a report and recommendations on ways to modernize the AML/CFT regulatory framework. In doing so, we will continue to consult with government, private sector, and civil society stakeholders. Our goal is also to take good, practical ideas and to find ways to implement those ideas as we continue to work on the overall report and recommendations. This information will inform the report to Congress required by Section 6216, as well as in other rulemakings and efforts in the coming months.

In parallel, we are spending considerable time on innovation and its implications for the AML/CFT regulatory framework. New technologies, automation of compliance efforts, and other innovations can all help to enhance implementation of AML/CFT programs. Our limited experience suggests that they may also allow financial institutions to allocate resources more efficiently and to engage in more high value, resource intensive investigative work that provides greater value to law enforcement.

For nearly three years, FinCEN has been using public-private engagement opportunities, such as our Innovation Hours program, to talk to financial institutions and FinTech or RegTech companies that are building innovative solutions.[12] These Innovation Hours allow FinCEN staff to learn about innovative solutions, better understand the degree to which financial institutions are deploying those solutions, and to ask questions about their regulatory implications.

We also continue to explore the creation of structured pilot programs. These can be frameworks for institutions to pilot the use of innovative technologies through exceptive relief authority. They do not have to be technology focused. For example, in accordance with Section 6212, we issued draft regulations on January 24, 2022, seeking comment on a pilot program for financial institutions to share SARs with their foreign affiliates: we received 17 comments.[13] In the

[11] *See* FinCEN, "FinCEN Seeks Comments on Modernization of U.S. AML/CFT Regulatory Regime," (December 14, 2021), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-modernization-us-amlcft-regulatory-regime

[12] *See* FinCEN, "FinCEN Announces Its Innovation Hours Program," (May 24, 2019), https://www.fincen.gov/resources/fincens-innovation-initiative.

[13] *See* FinCEN, "FinCEN Issues Proposed Rule for Suspicious Activity Report Sharing Pilot Program to Combat Illicit Finance Risk," (January 24, 2022), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-suspicious-activity-report-sharing-pilot-program

technology space, we can envision consideration of efforts involving artificial intelligence or machine learning-driven transaction monitoring, dynamic approaches to customer risk rating and institutional risk assessment, digital identity tools and utilities, and automating the adjudication and filing of SARs related to certain types of activity.

Enforcement and Compliance

Another cornerstone of our efforts to foster effective and efficient AML/CFT programs is enforcement and compliance. FinCEN is expanding its enforcement and compliance team and working closely, or in parallel, with the Federal Functional Regulators and law enforcement on compliance and enforcement efforts. Compliance examinations and enforcement actions play a critical role in driving broad compliance with the BSA.

As part of potentially extending and supplementing FinCEN's existing tools for regulatory guidance and relief, FinCEN is implementing the AML Act's no-action letter provision. This provision required FinCEN, in consultation with other agencies and officials, to conduct an assessment on whether to establish a process for the issuance of no-action letters in response to inquiries concerning the application of AML/CFT laws and regulations to specific conduct. It also required the Secretary, in coordination with others, to submit a report (the Report) to Congress, and propose rulemaking, if appropriate, to implement the findings.

FinCEN submitted and published the Report on June 28, 2021.[14] The Report concluded that FinCEN should undertake a rulemaking to establish a no-action letter process to supplement the existing forms of regulatory guidance and relief that may currently be requested from FinCEN. We aim to begin that rulemaking by publishing an ANPRM in the Federal Register this summer to solicit public comment on questions pertinent to the implementation of a no-action letter process at FinCEN.

FinCEN is also implementing the AML Act's whistleblower provisions, which are designed to pay awards to eligible individuals who have voluntarily provided FinCEN or the Department of Justice (DOJ) with original information about BSA violations. Funding constraints have slowed our efforts, but FinCEN has taken several steps to implement the whistleblower provisions. For example, in FY 2021, FinCEN created a new Office of the Whistleblower within its Enforcement and Compliance Division. We hired key personnel to build and lead the program. The office will eventually be staffed with a cadre of enforcement officers who will assess and investigate, where appropriate, whistleblower tips and information and process applications for awards.

FinCEN is actively reviewing tips and referring appropriate matters for investigation while drafting regulations to implement the whistleblower provisions of the AML Act in a way that encourages whistleblowers to step forward when they see or suspect BSA violations. These efforts include developing an online tip intake system and award application process. We are in the early stages of this effort, but we are very excited about it and look forward to the public

[14] *See* FinCEN, "FinCEN Completes Assessment on the Use of No-Action Letter," (June 30, 2021), https://www.fincen.gov/news/news-releases/fincen-completes-assessment-use-no-action-letters

comment following the publication of a Notice of Proposed Rulemaking, and working with Congress to further enhance this program.

Resources

While the AML Act made significant improvements to the AML/CFT framework, these improvements come at a cost. FinCEN employs a team of about 300 dedicated employees, including intelligence analysts, investigators, AML/CFT policy strategists, enforcement and compliance officers, outreach specialists, data analysts, regulators, and economists.

We appreciate the Fiscal Year (FY) 2022 appropriations to support the development of the beneficial ownership IT infrastructure and our efforts to support the U.S. response to Russian aggression. Nonetheless, FinCEN has significant staffing requests that remain unfunded. These include, but are not limited to, personnel needed to implement the beneficial ownership framework under the CTA, Foreign FIU Liaisons, Domestic Liaisons, BSA Innovation and Information Security Officers, enforcement officers for the new Whistleblower Office, other Enforcement and Compliance Division personnel, innovation experts, information security experts, data scientists and emerging technology experts, among other critical positions. Many of these positions are requirements of the AML Act.

The FY 2023 President's Budget request for FinCEN is $210.3 million—an increase of $49.3 million from the FY 2022 enacted levels. This request provides critical funding for AML Act and CTA implementation, including the full-time employees necessary to support on-going requirements from the AML Act, including the CTA, and FinCEN's Office of Chief Counsel more broadly.

Conclusion

In closing, timely and effective implementation of the AML Act, which includes the CTA, is a top priority. The FinCEN team is working diligently with law enforcement and regulatory stakeholders to promulgate rules and take other steps under the legislation that will further the national security of the United States and promote a more transparent financial system.

That said, limited resources have presented significant challenges to meeting the implementation requirements of our expanded mandate under the AML Act, including the CTA's beneficial ownership requirements. As you are aware, we are missing deadlines, and we will likely continue to do so. FinCEN's budget situation has required prioritization across the board, but we are working hard to meet our obligations. Congressional support for our FY 2023 budget request is critical to FinCEN's success in meeting AML Act requirements and general mission obligations.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.

FACTCOALITION
Financial Accountability & Corporate Transparency

April 28, 2022

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

RE: Virtual Hearing titled "Oversight of the Financial Crimes Enforcement Network"

Dear Chairwoman Waters and Ranking Member McHenry,

On behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition, we appreciate the opportunity to comment on your hearing titled, "Oversight of the Financial Crimes Enforcement Network." The FACT Coalition is a non-partisan alliance of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices.[1]

According to the U.S. Treasury Department, illicit proceeds equaling a staggering 2 percent of U.S. gross domestic product (GDP) move through our financial system each year.[2] As the inaugural 2021 U.S. Strategy to Counter Corruption noted, U.S. financial secrecy poses real dangers to average Americans, undermining public health, public safety, and national security.[3]

The Financial Crimes Enforcement Networks (FinCEN) has a critical role to play in addressing these dangers. FinCEN analyzes financial data to identify trends and help uncover illicit flows, provides support to law enforcement and national security officials to better investigate these cases, and implements structural reforms – such as those named in the U.S. Strategy on Countering Corruption – to prevent abuse of the U.S. financial system by the criminal and corrupt. The importance of this agency has only become clearer in light of U.S. sanctions against oligarchs allied with President Vladimir Putin in his illegal invasion of Ukraine.

Congress has a crucial oversight and appropriations role in empowering FinCEN to safeguard the U.S. financial system both effectively and efficiently.

[1] The FACT Coalition, "About Us," https://thefactcoalition.org/about-us/coalition-members-and-supporters/
[2] U.S. Treasury Department, "Treasury Strategic Plan 2022-2026," P. 23, March 2022, https://home.treasury.gov/system/files/266/TreasuryStrategicPlan-FY2022-2026.pdf.
[3] White House, "U.S. Strategy on Countering Corruption," December 2021, https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

The Corporate Transparency Act

In January 2021, Congress passed the bipartisan Corporate Transparency Act (CTA) – the most meaningful update to U.S. anti-money laundering laws in two decades, which would effectively end the abuse of anonymous shell entities by requiring certain entities to name their true, natural owner to a secure directory housed at FinCEN.

While we understand that FinCEN is diligently working to implement the law through three anticipated rulemakings, none of these three rulemakings have been finalized and two rules are yet to be proposed. Treasury Secretary Yellen committed in testimony before this committee on April 6 that the next rulemaking would be delivered "in the coming months."[4]

Congress should ask FinCEN to commit to standing up all final rules necessary to implement the CTA by no later than December 2022. Under the statute, rules implementing the CTA were to be promulgated by January 1, 2022. In order to be a credible host for December's International Anti-Corruption Conference (IACC) in Washington, the U.S. must finalize all rules for the CTA by the end of the year to demonstrate to the world that the U.S. is truly committed to tackling corruption. The urgency of creating this database has only become clearer in light of the current context of Russia's invasion of Ukraine.

We commend FinCEN for issuing a strong first draft rule defining beneficial ownership reporting requirements under the CTA, which hews closely to the statute and will yield meaningful disclosures from U.S. reporting entities. Still, **we encourage FinCEN to revise certain exemptions and resolve ambiguities around FinCEN identifiers in favor of transparency and efficiency, rather than secrecy inconsistent with the CTA**.[5]

Further, Congress should work with FinCEN ahead of the next rulemaking defining database access to ensure that authorized users have timely, uncomplicated, and complete access to the database in a manner consistent with the CTA, as this will be key to curbing the harmful practices associated with financial secrecy. Similarly, as the law allows foreign competent authorities to make requests of U.S. agencies for information in the database, **FinCEN should define access protocols in a way that facilitates international cooperation**, including in sanctions or human rights cases.[6]

---

[4] Janet Yellen, "The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System," Testimony before U.S. House Committee on Financial Services, April 6, 2022, https://financialservices.house.gov/events/eventsingle.aspx?EventID=409256

[5] The FACT Coalition, "Corporate Transparency Act's Draft Rule Applauded by FACT Coalition," February 8, 2022, https://thefactcoalition.org/corporate-transparency-acts-draft-rule-applauded-by-fact-coalition/

[6] The FACT Coalition, "RE: Beneficial Ownership Information Reporting Requirements," Comment to the Financial Crimes Enforcement Network, February 7, 2022, P. 88, https://thefactcoalition.org/wp-content/uploads/2022/02/FINCEN-2021-0005-0421_attachment_1.pdf

Finally, we encourage FinCEN to employ internationally accepted best data practices in collecting, storing, and making available to authorized users, beneficial ownership information subject to the CTA. FinCEN should, to the extent possible under the CTA, employ modern, internationally accepted data standards that were just endorsed in April by the Government of the United Kingdom. Congress should encourage FinCEN to create standardized forms and processes in connection with beneficial ownership information collection, including to ensure that data is verified upon submission and across other government databases in a way that makes it highly useful to authorized users and to keep costs low for businesses.. Additionally, FinCEN should be encouraged to employ machine readable data and systems designed with intergovernmental and industry use concerns top of mind. Congress should also encourage FinCEN to set up standardized access protocols to facilitate directory access by authorized users. Importantly, implementing the CTA and employing best data practices in doing so will also make the U.S. more current with recent revisions to beneficial ownership recommendations developed by the Financial Action Task Force (FATF), the international anti-money laundering standard setter.

OTHER CRUCIAL REVISIONS TO THE U.S. ANTI-MONEY LAUNDERING (AML) REGIME

Real Estate

According to a report by Global Financial Integrity, at least $2.3 billion has been laundered through U.S. real estate in the past 5 years. In 2002, the Treasury Department identified the real estate sector as an industry that would be required to stand up anti-money laundering programs, but then granted the sector a "temporary" exemption from meeting those obligations. Twenty years later, that exemption is still in place. Previously, FinCEN took important but inherently limited steps to stem money laundering in real estate. FinCEN is now reassessing the exemption in light of ongoing and consistent abuse of the real estate sector.[7]

Congress should urge FinCEN to finalize a nationwide rule that would require real estate professionals to have some AML/CFT obligation to understand their customers in the course of any residential or commercial real estate transaction, without cash thresholds.[8]

[7] Financial Crimes Enforcement Network, "Anti-Money Laundering Regulations for Real Estate Transactions," https://www.regulations.gov/document/FINCEN-2021-0007-0001/comment.
[8] The FACT Coalition, Submission to FinCEN Advanced Notice of Proposed Rulemaking. https://thefactcoalition.org/wp-content/uploads/2022/02/FACT-Final-RE-ANPRM-submission.pdf

Private Investment Funds

Treasury Secretary Yellen recommitted in her April 6 testimony that Treasury is "considering a rule that would address potential gaps in the AML/CFT for investment advisers,"[9] which was included in the Administration's Strategy on Countering Corruption. Like real estate, the private investment industry has also been temporarily exempted from risk-based AML/CFT for more than 20 years, but evidence of risks in the industry continue to mount.[10]

The $11 trillion U.S. private investment industry is large, opaque, and complex, making it the ideal destination for drug traffickers, corrupt officials, and rogue states alike to anonymously invest illicit proceeds.[11] In July 2020, a leaked FBI intelligence bulletin revealed that the FBI believed with ''high-confidence" that the U.S. private investment fund industry was being used to launder money.[12]

Congress should encourage FinCEN to undertake a timely rulemaking process and revise the 2015 draft rule to include registered investment advisers and unregistered investment companies. A rule should bring these individuals and entities into alignment with their counterparts in the U.S. financial system by requiring them to stand up basic risk-based AML programs, identify true beneficial owners of entity customers and investors, file Suspicious Activity Reports (SARs) with FinCEN, and maintain accurate records.

Risk-Based AML Approach Among Financial "Gatekeepers"

The new United States Strategy on Countering Corruption marks the Administration's intention to bring key "gatekeepers" to the U.S. financial system under the purview of U.S. anti-money laundering laws.[13] As these professions are situated to create and direct hidden wealth through the U.S. financial system through opaque entities or other modalities on behalf of their clients,

---

[9] Janet Yellen, "The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System."

[10] See e.g., Todd C. Frankl, The search for oligarchs' wealth in U.S. is hindered by investment loopholes, Washington Post (Mar. 16, 2022), https://www.washingtonpost.com/business/2022/03/16/private-equity-regulation-gap/.

[11] FACT Coalition, Global Financial Integrity, and Transparency International-US Office, "Private Investments, Public Harm: How the Opacity of the Massive U.S. Private Investment Industry Fuels Corruption and Threatens National Security," December 2, 2021, https://thefactcoalition.org/report/private-investments-public-harm/.

[12] FACT Coalition, Global Financial Integrity, and Transparency International-US Office, "Private Investments, Public Harm: How the Opacity of the Massive U.S. Private Investment Industry Fuels Corruption and Threatens National Security."
See also Timothy Lloyd, "FBI concerned over laundering risks in private equity, hedge funds - leaked document," Reuters, July 14, 2020, https://www.reuters.com/article/bc-finreg-fbi-laundering-private-equity/fbi-concerned-over-laundering-risks-in-private-equity-hedge-funds-leaked-document-idUSKCN24F1TP

[13] U.S. White House, "United States Strategy on Countering Corruption," December 6, 2021, p. 23, https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.

this would be a key step to ensure criminals and corrupt officials are denied financial safe haven in the United States.

The Financial Services Committee has noticed a discussion draft the "Transparency and Accountability in Service Providers Act". This legislation would take a risk-based approach to countering money laundering risk by requiring certain "gatekeepers" to the U.S. financial system to adopt procedures to help detect, flag, and prevent the laundering of corrupt and other criminal funds into the United States.

Congress should work with FinCEN and the Treasury Department to advance legislation, like the Transparency and Accountability in Service Providers Act that was noticed for this hearing as a discussion draft, to help close these long-standing gaps in safeguards for the U.S. financial system.

Digital Assets

FinCEN has engaged in efforts to incorporate cryptocurrency and other digital assets into existing anti-money laundering regimes, including through proposed regulations promulgated and most recently extended in January of 2021.[14] We encourage FinCEN to make clear that cryptocurrency and digital assets are subject to current anti-money laundering rules, to further rulemakings that address specific risks associated with technologies capable of avoiding traditional third-party reporting regimes. **Congress should encourage FinCEN to avoid creating any loopholes or exemptions within the U.S. anti-money laundering framework on the basis of incentivizing a "novel" technology or otherwise.**

FinCEN Appropriations

In the Administration's inaugural Strategy on Countering Corruption, FinCEN plays a leading role in bringing U.S. anti-money laundering (AML) laws into the 21st century. Yet FinCEN – tasked with safeguarding the world's largest economy – currently has half of the staff of the analogous financial intelligence unit in Australia, which has an economy less than 1/15th the size of that of the United States.

The President's budget request of $210.3 million for FY2023 is essential to enable the agency to enact necessary U.S. AML reforms. Congress should consider this a floor, not a ceiling, on funding for the agency.

[14] Financial Crimes Enforcement Network, "FinCEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions," January 14, 2021, https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering

Enacted levels for FY2022 appropriations fell $30 million short of the Administration's discretionary request. The national security implications – whether the urgent case of responding to Russia's war in Ukraine, or the long-term vulnerabilities of our lacking financial safeguards – warrant appropriations that exceed the President's request, to make the agency whole for $240.3 million. **Congress should appropriate a total of $240.3 million for FY2023 for FinCEN**.

CONCLUSION

Thank you for your time. If you have any questions, you can contact Erica Hanichak (ehanichak@thefactcoalition.org).

Sincerely,

Ian Gary
Executive Director

Erica Hanichak
Government Affairs Director

Ryan Gurule
Policy Director

PROJECT ON GOVERNMENT OVERSIGHT

Statement of Joanna Derman, Policy Analyst
Project On Government Oversight
Before the House Financial Services Committee
On "Oversight of the Financial Crimes Enforcement Network"
April 28, 2022

Chairwoman Waters, Ranking Member McHenry, and members of the committee, thank you for the opportunity to submit a statement for the record regarding the critical role that the Financial Crimes Enforcement Network (FinCEN) plays in protecting the U.S. economy from financial crimes, and the importance of FinCEN's swift implementation of the Corporate Transparency Act (CTA).

I am Joanna Derman, policy analyst at the Project On Government Oversight (POGO). POGO is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

FinCEN is the bureau of the Treasury Department specifically tasked with the enormous responsibility "to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."[1]

FinCEN plays a crucial role in protecting the U.S. economy from foreign malign influence. To that end, it is a leading financial intelligence unit and coordinates widely with international partners to share and exchange financial information in support of U.S. and foreign financial crime investigations.[2] FinCEN is also a lead implementing agency for the reforms listed in President Joseph Biden's December 2021 inaugural strategy on countering corruption.[3]

Recently, FinCEN has been widely discussed within the context of combatting Russian aggression against Ukraine, as the bureau endeavors to remain vigilant against potential efforts to evade the robust sanctions regime that the U.S. and our allies recently expanded with respect to both the Russian Federation and individual Russian oligarchs.[4] As you, Chairwoman Waters,

---

[1] Financial Crimes Enforcement Network, "Mission," accessed April 25, 2022, https://www.fincen.gov/about/mission.
[2] Financial Crimes Enforcement Network, "What We Do," accessed April 25, 2022, https://www.fincen.gov/what-we-do.
[3] The White House, *United States Strategy on Countering Corruption* (December 2021), 19, https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf.
[4] The FACT Coalition, "Now is the Time to Modernize FinCEN: Just the FACTS: April 8," April 8, 2022, https://thefactcoalition.org/now-is-the-time-to-modernize-fincen-just-the-facts-april-8/; Mengqi Sun, "Russian Kleptocrats of Particular Concern to U.S. Treasury," *Wall Street Journal*, April 14, 2022,

recently noted, bad actors in Russia "are using shell companies and other money laundering techniques to hide their money, avoid scrutiny, and evade our sanctions."[5] These actions shine a spotlight on what financial regulators have known for a long time: that kleptocrats and criminals have consistently taken advantage of gaps in the framework protecting western financial economies in order to hide their wealth from prying eyes.[6] For example, last month Russian oligarch Roman Abramovich, who is subject to international sanctions, docked his two super yachts in Turkey. With each yacht worth an estimated $600 million or more, he is literally moving his money around the world while he seeks to outrun their capture.[7] As another example, Russian oligarch Oleg Deripaska, who has been sanctioned by the U.S. since 2018, has reportedly used anonymous shell companies and proxies to secretly own real estate in the U.S. to this day, without fear of seizure.[8] In another instance, in 2016, Russian oligarch Igor Makarov established an unregulated private trust company in Wyoming to anonymously grow and hide his wealth in the U.S financial system.[9] FinCEN must continue to work with our international allies to close these loopholes in our financial system and finally bring these individuals to account.

Ensuring Increased FinCEN Fundings

Given the critical role that FinCEN plays in protecting the security of our nation's financial systems, Congress should not hesitate to significantly increase FinCEN's funding and fulfill President Biden's fiscal year 2023 budget request of $210 million for FinCEN.[10] With all eyes on anti-corruption efforts targeting Russian oligarchs, lawmakers must recognize that in order for FinCEN to produce meaningful enforcement efforts, they must be afforded at least the minimum amount of resources they need for staffing, technology, licensing, travel, and other operational necessities.

In fiscal year 2022, Congress unfortunately fell $30 million short of President Biden's request of $191 million for FinCEN.[11] While the resultant $161 million for FinCEN that fiscal year

---

https://www.wsj.com/articles/russian-kleptocrats-of-particular-concern-to-u-s-treasury-11649974520; Katy O'Donnell, "Oligarchs' big loophole for stashing money," *Politico*, April 11, 2022, https://www.politico.com/news/2022/04/11/washington-poised-to-clamp-down-on-oligarchs-real-estate-00023347.

[5] House Financial Services Committee, "Waters Opening Statement at March Full Committee Markup on Bipartisan Bills to Punish Russia and Support Ukraine," Press Release, March 17, 2022, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409203.

[6] Katy O'Donnell, "Oligarchs' big loophole for stashing money," *Politico*, April 11, 2022, https://www.politico.com/news/2022/04/11/washington-poised-to-clamp-down-on-oligarchs-real-estate-00023347.

[7] Karen Gilchrist, "Russian oligarch Abramovich's two superyachts worth a combined $1 billion are escaping sanctions – for now," CNBC, March 24, 2022, https://www.cnbc.com/2022/03/24/russia-oligarch-abramovichs-superyachts-evade-sanctions.html.

[8] Roman Goncharenko, "The Russian oligarchs of the FinCEN Files," *Deutsche Welle*, September 26, 2020, https://www.dw.com/en/the-russian-oligarchs-of-the-fincen-files/a-55062675.

[9] Will Fitzgibbon and Debbie Cenziper, "The 'cowboy cocktail': How Wyoming became one of the world's top tax havens," International Consortium of Investigative Journalists, December 20, 2021, https://www.icij.org/investigations/pandora-papers/the-cowboy-cocktail-how-wyoming-became-one-of-the-worlds-top-tax-havens/.

[10] Office of Management and Budget, *Budget of the U.S. Government, Fiscal Year 2023* (March 2022), 98, https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf.

[11] House Committee on Appropriations, "H.R. 2471, Funding for the People, Division-by-Division Summary of Appropriations Provisions," 16 [page in PDF], https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/Appropriations%20Division-by-

constituted an increase from the prior fiscal year, it is clear that FinCEN is still in need of additional resources in order to fulfill its mission.

Congress must do better. Lawmakers should fully and consistently fund FinCEN, especially as Congress continues to expand FinCEN's mandate, most recently in 2021 through the Anti-Money Laundering Act of 2020. The act added substantial responsibilities to FinCEN's plate and highlighted certain factors that FinCEN needs to consider when prescribing the compliance framework for combatting money laundering and financial terrorism.[12]

FinCEN Must Swiftly Implement the Corporate Transparency Act

Signed into law on January 1, 2021, the Corporate Transparency Act (CTA) requires corporations, limited liability companies, and similar entities to report their true beneficial owners to FinCEN, and directs FinCEN to house and maintain this information in a central registry so authorized law enforcement and financial institutions can use it to crack down on criminal and illicit financial exchanges and money laundering.[13]

FinCEN should fully and expeditiously implement the CTA. Currently, the Treasury Department is beyond its statutory timeframe of one year to implement the law. It has been in the process of implementing the CTA for the past year, issuing the first of what will be three Notices of Proposed Rulemaking in December 2021.[14] Treasury Secretary Janet Yellen said before this committee on April 6, 2022, that the Treasury Department expects a second rule "this year, within the coming months."[15]

POGO encourages the Treasury Department to see through its commitment to this schedule, and urges the department to ensure that CTA implementation be finalized and take effect no later than January 1, 2023. The administration should move to quickly issue the second and third proposed rulemakings for the CTA, and to make effective final regulations.

POGO recently submitted an appropriations request to that effect to Congress, requesting reporting language that encourages the Treasury Department to swiftly implement the CTA.

Division%20Summary.pdf; Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[12] Himamauli Das, "Prepared Remarks of FinCEN Acting Director Himamauli Das During NYU Law's Program on Corporate Compliance and Enforcement," (speech, New York University School of Law, March 25, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-himamauli-das-during-nyu-laws-program.

[13] 31 U.S.C. § 5336(b)(4)(B)(ii).

[14] Beneficial Ownership Information Reporting Requirements, 86 Fed. Reg. 69,920-69,974 (proposed December 8, 2021), https://www.federalregister.gov/documents/2021/12/08/2021-26548/beneficial-ownership-information-reporting-requirements; Beneficial Ownership Reporting Requirements, 86 Fed. Reg. 17,557-17,565 (proposed April 5, 2021), https://www.govinfo.gov/content/pkg/FR-2021-04-05/pdf/2021-06922.pdf.

[15] *The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System: Hearing before House Financial Services Committee*, 117th Cong. (April 6, 2022) (testimony of Treasury Secretary Janet Yellen), 2:52:37, https://www.youtube.com/watch?v=dOrFipJ4qt8.

Priorities in CTA Rulemaking

In response to the Treasury Department's CTA rulemaking process, POGO submitted two comments, both of which are enclosed in this document and include recommendations on how to implement the law most effectively.

First, POGO submitted a comment to the Treasury Department's Advanced Notice of Proposed Rulemaking published in the federal register on April 5, 2021.[16] We recommended that FinCEN adhere closely to the statutory language in the CTA, paying close attention to how accessible the beneficial ownership database is to law enforcement. For the database to be as "accurate, complete, and highly useful" as possible, FinCEN must craft the database in a manner that allows for timely access to information and push for the use of unique, non-proprietary identifiers for each company in the database to make it easier to monitor and track illicit transactions.

Second, POGO submitted a comment to the Treasury Department's Notice of Proposed Rulemaking published in the federal register on December 8, 2021.[17] We recommended that FinCEN retain its strong definitions of both a reporting company and a beneficial owner, retain its proposed reporting requirements, and retain its efforts to minimize cost of compliance. Additionally, we recommended that FinCEN clarify the exemption policy for subsidiaries of reporting companies, require mandatory Legal Entity Identifier numbers, and take additional steps to strengthen the accuracy and usefulness of reported information.

We look forward to reviewing FinCEN's forthcoming rule regarding the CTA.

Conclusion

POGO is grateful to the committee for holding this important hearing, and we urge you to act to increase FinCEN funding, swiftly implement the CTA, and continue to take concrete steps that ensure bad actors are unable to make illicit financial transactions that harm our national security.

Sincerely,

Joanna Derman

Joanna Derman
Policy Analyst

Enclosures: 2

[16] Tim Stretton, "POGO Submits Comment on Creation of New Federal Beneficial Ownership Database," Project On Government Oversight, May 5, 2021, https://www.pogo.org/letter/2021/05/pogo-submits-comment-on-creation-of-new-federal-beneficial-ownership-database/.
[17] Joanna Derman, "POGO Submits Second Comment on Creation of New Beneficial Ownership Database," Project On Government Oversight, February 7, 2022, https://www.pogo.org/letter/2022/02/pogo-submits-second-comment-on-creation-of-new-federal-beneficial-ownership-database/.

PROJECT ON GOVERNMENT OVERSIGHT

May 5, 2021

AnnaLou Tirol
Deputy Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Submitted via the Federal E-rulemaking Portal at http://www.regulations.gov

Subject: Comment in response to Proposed Rulemaking: Beneficial Ownership Information Reporting Requirements, Docket Number FINCEN-2021-0005; RIN 1506-AB49

Dear Deputy Director Tirol:

The Project On Government Oversight (POGO) submits the following comment in response to the request by the Financial Crimes Enforcement Network (FinCEN) for comment on an advance notice of proposed rulemaking, published in the Federal Register on Monday, April 5, 2021.[1] The final rule that results will implement the beneficial ownership reporting requirements mandated by the Corporate Transparency Act. We appreciate the opportunity to weigh in on this important rulemaking.

POGO is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

Good government reform must include the collection of accurate information on the individuals who really own, and benefit financially from, companies—known as beneficial ownership information. Investigations into waste, fraud, and abuse in government spending have routinely found companies with anonymous or opaque ownership structures to be dangerous facilitators of corruption and misconduct. The language in the Corporate Transparency Act makes monumental progress in increasing transparency in corporate structures in the United States.

Beneficial Ownership Database

The Corporate Transparency Act requires companies formed in the U.S., with some exceptions, to disclose information about their beneficial owners to law enforcement and financial institutions such as banks. The law's definition of beneficial ownership is strong. The Treasury

[1] Beneficial Ownership Information Reporting Requirements, 86 Fed. Reg. 17,557-17,565 (proposed April 5, 2021). https://www.govinfo.gov/content/pkg/FR-2021-04-05/pdf/2021-06922.pdf

Department's Financial Crimes Enforcement Network, or FinCEN, will collect and house companies' beneficial ownership information in a secure nonpublic database.[2] The agency is uniquely qualified to oversee beneficial ownership information, as its stated mission is to "safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[3]

When creating the database and the rules governing its use, FinCEN should adhere closely to legislative intent. Congress carefully crafted the Corporate Transparency Act in a way that would be useful to law enforcement and financial institutions in the effort to combat illicit financial transactions and to protect national security. For the database to be a valuable resource, FinCEN must ensure law enforcement entities have timely access to information in the database and must use unique, non-proprietary identifiers for each company to make it easier to track illicit transactions.

Timely Access to Information

While the law has ensured that the business information in FinCEN's database will not be publicly available, local, state, federal, and in some cases international law enforcement entities will be able to access it to support ongoing investigations. Allies overseas should be able to access the information through appropriate protocols such as mutual legal assistance treaties and other agreements. In order for the database to be as useful as intended, the rule should ensure that all law enforcement entities have timely access to the database.

The rule should define law enforcement activities as broadly as possible to include criminal, civil, and administrative enforcement duties. Doing so will make it easier for law enforcement entities to quickly access information that may be helpful to ongoing investigations. On the other side of the coin, creating a narrow definition risks preventing law enforcement entities from accessing information in the database, which could harm those investigations.

In addition, the rule should make clear who has the authority to approve and deny requests for database information. This will improve efficiency and protect the integrity of the database by reducing the risk of unauthorized approval. The rule should also make clear what positions at law enforcement entities have the authority to request information.

Another issue the rule should address is the likelihood that law enforcement entities will need information about multiple individuals in a case. FinCEN should adopt certification procedures for law enforcement investigations and, once that investigation is approved for access to information, the certification should remain valid for the duration of the investigation. A process that would require an entity to obtain certification for each information request in an investigation would severely increase the time it takes law enforcement to get the information they need. The system should also permit the entity to submit their certification materials at the

[2] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong., § 6401(7)(A) (2021). https://www.congress.gov/bill/116th-congress/house-bill/6395/text
[3] "What We Do," Financial Crimes Enforcement Network. https://www.fincen.gov/what-we-do (accessed on April 22, 2021)

same time they submit the information request, which will reduce transaction time. In addition, once a law enforcement entity is approved to access the database for a particular investigation, FinCEN should allow that organization to submit one request for multiple people related to the investigation if needed, rather than requiring them to submit separate requests for each person of interest. This fast-tracked approach will reduce administrative burden and facilitate the timely sharing of information that is necessary to help protect national security, intelligence gathering, and law enforcement.

Finally, foreign law enforcement entities should be able to access certain information when appropriate. The illicit flow of money is a global problem that has serious implications for U.S. national security. Anonymous companies facilitate a wide variety of illicit activities that directly harm U.S. foreign policy interests, finance terrorism, and enable sanctions evasion. In situations where there are existing mutual legal assistance treaties and other law enforcement cooperation agreements between a country and the United States, law enforcement entities in those countries should be able to quickly access needed information. FinCEN should also work with federal agencies at various attaché offices abroad so they are familiar with the database in case it could help in their investigations. Opaque corporate ownership is an international problem, and swift international cooperation will be key to making the United States and the world safer.

Unique Identifiers

The Corporate Transparency Act requires that FinCEN issue a "FinCEN identifier" to an individual or entity that has submitted the required beneficial ownership information.[4] When deciding what identifier to use, FinCEN should ensure it is a non-proprietary system, such as the global Legal Entity Identifier (LEI) system. The LEI is a 20-character, alpha-numeric code that enables clear and unique identification of legal entities participating in financial transactions.[5] Given resource constraints, FinCEN could even consider contracting with the Global Legal Entity Identifier Foundation to provide the unique identifiers. The foundation assigns a number to any type of legal entity requesting one. Regardless of whether FinCEN chooses to create its own identifier system or to use an existing one, the unique entity identifier should be non-proprietary and should link all domestic and foreign relationships, including parents, subsidiaries, joint ventures, partnering arrangements, and mentor programs.

In order for the FinCEN database to be as useful as possible in combating illicit money flows, it needs to be complete and accurate. For that to happen, companies need to be able to enter required information with ease, and in a way that prevents errors or incorrect information from being introduced into the system. To that end, the new identifier system must have instant verification mechanisms built in to ensure the use of a company's correct identifier. Such mechanisms need to be triggered immediately so that entities submitting information cannot submit out-of-date identifiers or be issued new and unnecessary identifiers. This is a process that's widely used in the private sector, such as when a credit card company declines a consumer's transaction if the billing information the customer enters doesn't match what the

[4] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong., § 6403(a) (2021). https://www.congress.gov/bill/116th-congress/house-bill/6395/text
[5] "Introducing the Legal Entity Identifier (LEI)," Global Legal Entity Identifier Foundation https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei (accessed on April 25, 2021).

company has on file. Similarly, if someone enrolled in the Transportation Security Administration's PreCheck program tries to book a flight but enters a different Known Traveler Number than what the agency has on file, the flight cannot be booked. Imagine if you found out days or weeks later that your online order was declined or your flight wasn't booked because you entered the wrong information, rather than being informed immediately? It would be beyond frustrating and not just a minor inconvenience. For businesses this extra time it takes to go through the whole process again is time lost—which is money lost.

As companies try to comply with the law and register their beneficial owners, it is imperative that the process be as minimally burdensome as possible. This is especially important for small businesses. Creating instant verification mechanisms will help these companies register correctly the first time, rather than being forced to come back and do it all over again because of a typo or other registration error. If the process is easy for businesses, especially small businesses, they will be much more likely to comply.

Conclusion

Companies with hidden anonymous ownership structures are a serious global problem, and in many instances those entities are involved in international corruption that doesn't stop at the U.S. border. These anonymous shell companies facilitate a wide variety of illicit activities that directly harm U.S. foreign policy interests and national security. The Corporate Transparency Act mandated a beneficial ownership database that will enable law enforcement and bank officials to learn more about the true owners of companies. This information will help the officials root out corruption, fraud, and illicit financial transactions, and ensure that taxpayer dollars are going to law-abiding contractors and grantees rather than to companies engaging in fraud or posing national security risks. FinCEN's database will be key to the success of this effort.

Thank you for your consideration of this comment. Should you have any questions, please contact me at tstretton@pogo.org.

Sincerely,

Tim Stretton
Policy Analyst

February 4, 2022

Himamauli Das
Acting Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Submitted via the Federal E-Rulemaking Portal at http://www.regulations.gov

Subject: Proposed Rulemaking: Beneficial Ownership Information Reporting Requirements, Docket Number FINCEN-20210-0005, RIN 1506-AB49

Dear Acting Director Das:

This comment responds to the Financial Crimes Enforcement Network's (FinCEN) notice of proposed rulemaking on beneficial ownership information reporting requirements, published in the Federal Register on December 8, 2021,[1] to implement the Corporate Transparency Act (CTA). We appreciate the opportunity to weigh in on this important rulemaking.

The Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

Good government reform must include the collection of certain information regarding the ownership of anonymous shell companies — known as beneficial ownership information — including the identity of companies' true, natural owners. Right now, to the detriment of the American taxpayer, it is all too easy for corrupt actors who own and profit from companies to hide their true identities behind layers of anonymous ownership structures for the purpose of facilitating illicit financial transactions.

With some exceptions, the Corporate Transparency Act requires companies that are formed in or registered to do business in the U.S. to disclose and keep up to date such beneficial ownership information to the federal government in an "accurate, complete, and highly useful" manner.[2] According to the Corporate Transparency Act, this beneficial ownership information shall then

[1] Beneficial Ownership Information Reporting Requirements, 86 Fed. Reg. 69,920-69,974 (proposed December 8, 2021), https://www.federalregister.gov/documents/2021/12/08/2021-26548/beneficial-ownership-information-reporting-requirements.
[2] 31 U.S.C. § 5336(b)(4)(B)(ii).

be housed in a secure database and made available to national security, intelligence, and law enforcement agencies; foreign law enforcement via request with a U.S. agency; and certain financial institutions, such as banks, that have customer due diligence obligations for the purposes of combatting financial corruption, misconduct, and a wide variety of illicit activities that harm U.S. national security.[3]

POGO applauds this draft rule and sees it as important progress toward modernizing the U.S. anti-money laundering framework, as well as a key opportunity to protect the U.S. financial system from abuse by criminal and corrupt actors.

Consistent with POGO's May 5, 2021, recommendations submitted in response to FinCEN's Advanced Notice of Proposed Rulemaking, the Department of the Treasury crafted this rule in a way that adheres closely to the statutory language in the Corporate Transparency Act, implements key aspects of the statute, and offers meaningful transparency into the real, natural owners behind a range of legal entities operating in the U.S.[4]

In order to make this beneficial ownership database as "accurate, complete, and highly useful" as possible, POGO recommends retaining this rule's faithful definition of a reporting company, its strong definition of a beneficial owner (absent the language surrounding senior officers, clarified below), its timely reporting requirements, and its efforts to minimize cost of compliance for covered entities. POGO also recommends clarifying the exemption for subsidiaries of reporting companies (known as exemption 22), requiring mandatory Legal Entity Identifier (LEI) numbers, and imposing additional verification mechanisms on the database.

Faithful Definition of a "Reporting Company"

With respect to the definition of a "reporting company," the Corporate Transparency Act requires corporations, limited liability companies, and "other similar entities" to disclose beneficial ownership information to the federal government. In FinCEN's proposed rule, the Treasury Department defines the term "other similar entities" as any entity that was either created under the laws of the state or Indian tribe, or that registered to do business in the state or tribal jurisdiction, by filing a document with a secretary of state or similar office.[5] The draft rule states that its definition would "likely include limited liability partnerships, limited liability limited partnerships, business trusts … and most limited partnerships, in addition to corporations and limited liability companies (LLCs)," as they also typically file with a state secretary or other similar office.[6]

This process-oriented definition of a reporting company provides flexibility that accounts for the filing practices unique to each state. For example, as noted by Transparency International's U.S. office, if a particular state determines that a trust not otherwise exempted by the Corporate

[3] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong., § 6401(7)(A) (2021), https://www.congress.gov/bill/116th-congress/house-bill/6395/text.
[4] Project On Government Oversight, Comment Letter on Proposed Rule on Creation of New Federal Beneficial Ownership Database (May 5, 2021), https://www.pogo.org/letter/2021/05/pogo-submits-comment-on-creation-of-new-federal-beneficial-ownership-database/.
[5] Beneficial Ownership Information Reporting Requirements (proposed December 8, 2021) [see note 1].
[6] Beneficial Ownership Information Reporting Requirements (proposed December 8, 2021) [see note 1].

Transparency Act must be formed through filing documents with its secretary of state, that trust will be covered under the definition of a reporting company and be required to report its beneficial ownership information to the secure directory.[7]

The definition of a reporting company in FinCEN's draft rule will help meet the Corporate Transparency Act's mandate that information provided to the directory be "highly useful,"[8] as it will help law enforcement identify the true natural owner behind a variety of U.S. legal entities, which are often interchanged in complex ownership structures. While risks still exist, the process-oriented approach reduces certain risks of driving demand for other, more opaque methods of obscuring beneficial ownership information.[9] FinCEN should work with states to ensure new vulnerabilities are not created in the wake of the Corporate Transparency Act's implementation.

Strong Definition of "Beneficial Owner"

As POGO has previous noted, the Corporate Transparency Act's definition of a "beneficial owner" is strong.[10] According to the law, a beneficial owner of an entity, subject to certain exceptions, is an individual who either owns no less than 25% of the ownership interests of the entity or who exercises "substantial control over the entity."[11] The term "substantial control" was not further defined in the Corporate Transparency Act. Leading up to its call for comments for the May 2021 Advanced Notice of Proposed Rulemaking, the Treasury Department even considered whether or not to interpret the term "substantial control" to mean that no entity could have more than one beneficial owner who is listed as exercising "substantial control" of an entity, which would have severely limited the utility of the database.[12]

In contrast, FinCEN's draft rule requires the naming of one or multiple owners that meet the proposed definition of a beneficial owner and identifies several types of individuals who shall be considered to exercise substantial control. This list is non-exhaustive, and includes but is not limited to: individuals who serve as a senior officer of the reporting company, individuals who have authority over the appointment or removal authority within the entity, and "any other form of substantial control over the reporting company."[13]

One place where FinCEN can improve upon its proposed list is its usage of the term "senior officer." Senior officers are often simply higher-ranking employees in a company who do not

---

[7] Transparency International, "Four Initial Takeaways from the Draft CTA Rule," https://us.transparency.org/resource/four-initial-takeaways-from-the-draft-corporate-transparency-act-rule/.
[8] 31 U.S.C. § 5336(b)(4)(B)(ii).
[9] Studies of the implementation of the U.K.'s beneficial ownership registry showed that the incorporation of a relatively unpopular corporate entity — the Scottish limited partnership — jumped between 2015 and 2016. Their numbers dwindled shortly after the U.K. included them in the definition of reporting entity. Nienke Palstra, "Three Ways in Which the U.K.'s Register of the Real Owners of Companies is Already Proving its Worth," Global Witness, July 24, 2018, https://www.globalwitness.org/en/blog/three-ways-uks-register-real-owners-companies-already-proving-its-worth/.
[10] Project On Government Oversight, Comment Letter on Proposed Rule [see note 4].
[11] 31 U.S.C. § 5336(b)(4)(B)(ii).
[12] Transparency International, "Four Initial Takeaways from the Draft CTA Rule" [see note 7].
[13] Transparency International, "Four Initial Takeaways from the Draft CTA Rule" [see note 7]; Beneficial Ownership Information Reporting Requirements (proposed December 8, 2021) [see note 1].

exercise any authority over the operations of the entity. As such, senior officers should be more carefully defined such that the term only describes those senior officers who hold substantive control over a company. Separately, this catch-all language related to "any other form of substantial control" is important, because it would capture a wide spectrum of illicit actors, including those who exert control through illicit methods, such as instances of bribery or threats.

With the minor exception of the language concerning senior officers, FinCEN's draft rule should retain the proposed definition of substantive control. This would ensure that all relevant information is appropriately collected and housed in the beneficial ownership database and made accessible to law enforcement and appropriate financial institutions.

Timely Reporting Requirements

The Corporate Transparency Act requires the Treasury Department to define two central terms with respect to when reporting entities must submit beneficial ownership information to the federal government. First, the law states that a covered entity must report its beneficial ownership information "at the time of formation or registration," but does not further specify what timeframe this must entail. Second, the law stipulates that if an entity must update its beneficial ownership information, it must do so in a timely manner that does not exceed a year after the date on which the change occurs, but it does not further specify what a "timely manner" means.[14]

In FinCEN's proposed rule, the Treasury Department interpreted the terms "at the time of" and "in a timely manner" to mean within 14 days and within 30 days, respectively. As stated by Transparency International's U.S. office, this is in line with beneficial ownership directories in France and Luxembourg.[15] Aligning this registry with international standards could potentially make it easier to work with allies in cross-border efforts to combat money laundering and corruption. Furthermore, this rule specifies that if an exempted entity loses its exempted status, it has 30 days to report its beneficial ownership information to the proper authorities.[16] These timeframes for reporting are extremely reasonable, and balance what can be practicably expected of an entity with rational expectations surrounding the utility of the beneficial ownership database.

Low Cost of Compliance

In compliance with the statute, the draft rule minimizes the costs to businesses by keeping the cost of compliance for reporting companies low. According to Deputy Secretary Wally Adeyemo, the Treasury Department estimates that the cost of compliance, on average, will be less than $50 per company.[17]

---

[14] National Defense Authorization Act for Fiscal Year 2021, § 6401(7)(A) [see note 3].
[15] Transparency International, "Four Initial Takeaways from the Draft CTA Rule" [see note 7].
[16] Transparency International, "Four Initial Takeaways from the Draft CTA Rule" [see note 7].
[17] U.S. Department of the Treasury, "Remarks by Deputy Secretary of the Treasury Wally Adeyemo on Anti-Corruption at the Brookings Institution," December 6, 2021, https://home.treasury.gov/news/press-releases/jy0516.

After implementing its own directory, the government of the U.K. surveyed covered companies and found that companies with fewer than 50 employees reported ongoing costs of just over $5 on average.[18] It is reasonable to expect similar outcomes in the U.S., where small firms ("mom and pop" style enterprises, for example) have simple ownership structures that are easy to identify and update at the time of any changes. On the other hand, small firms with enough resources to set up more costly, complex ownership structures would almost certainly have the resources necessary to identify and name to FinCEN their true, natural owner. In light of the data from the U.K.'s own directory, FinCEN's draft rule should reassess the cost-benefit analysis to account for the minimal anticipated costs to keep current with disclosures after the initial implementation of the Corporate Transparency Act rule.

Clarifying the Exemption for Subsidiaries of Reporting Companies (Exemption 22)

The Corporate Transparency Act exempts nearly two dozen different types of entities from the definition of a reporting company, including but not limited to: securities issuers, domestic governmental authorities, banks, domestic credit unions, depository institution holding companies, and money transmitting businesses. Aside from a select number of proposed clarifications, FinCEN's proposed rule declines to add exemptions, and instead adopts the statutory language granting these 23 exemptions verbatim from the Corporate Transparency Act, which is in line with POGO's preference to adhere as closely as possible to legislative intent.

One area for improvement in the proposed rule is exemption 22, which states that companies are exempt from reporting their beneficial ownership information if "the[ir] ownership interests are controlled or wholly owned, directly or indirectly" by one or more exempt entities.[19]

As written in the rule, exemption 22 presents a major oversight loophole for these subsidiary companies. By exempting subsidiaries that are simply "controlled," as opposed to "wholly controlled," by exempted entities, the rule would incentivize bad actors to seek out exempted companies to serve as a majority owner or partner in a joint venture in order to evade detection. This approach would also expand the universe of entities exempted from submitting their beneficial ownership information. Taken together, this exemption would fail to capture potentially illicit actors and allow them to continue concealing their identity behind anonymous shell companies.

The Treasury Department should revise the rule by narrowing the proposed exemption 22 language of "controlled or wholly owned" to "*wholly* controlled or wholly owned," which would explicitly articulate that only entities whose entire ownership interests are owned or controlled by an exempt entity may be exempted from disclosing beneficial ownership information.

Improving Efficiency Through Mandatory Legal Entity Identifiers

---

[18] U.K. Department for Business, Energy & Industrial Strategy, *Review of the implementation of the PSC Register*, BEIS Research Paper Number 2019/005 (March 2019), 23, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822823/review-implementation-psc-register.pdf.

[19] Beneficial Ownership Information Reporting Requirements (proposed December 8, 2021) [see note 1].

FinCEN's rule should require covered entities to submit mandatory Legal Entity Identifier (LEI) numbers. LEI is a 20-character alpha-numeric code that is intended to enable law enforcement and financial institutions to clearly see "who is who" and "who owns whom."[20] LEIs are commonly used in the U.S. and are being adopted as a global standard in business transactions. According to FinCEN's proposed rule, over 244,000 entities in the U.S. already use LEIs to identify and distinguish themselves from other entities.[21]

LEI numbers would not only provide an additional way to verify the information submitted to the registry, but would also simplify information collection, storage, and access across international lines, since LEIs can be assigned internationally. Also, the LEI system is nonproprietary, and therefore is not limited by restrictions placed on it by its parent company, and is subject to transparency requirements such as the Freedom of Information Act. This would mitigate concerns expressed by nonprofit organization OMB Watch that proprietary systems are not subject to such transparency, and could pose oversight challenges for auditors or groups seeking to independently determine the accuracy or comprehensiveness of the information collected.[22] Additionally, LEIs must be renewed annually, which adds another layer of security.

With respect to registering entities with the beneficial ownership database, obtaining a unique identifier should be simple, comprehensive, and as minimally burdensome as possible, especially for small businesses.

Separately, according to the Corporate Transparency Act, FinCEN may issue a unique identifier upon request, referred to as a FinCEN identifier, to an individual or entity that submits the required beneficial ownership information.[23] We propose that the rule should make it mandatory for FinCEN to issue a FinCEN identifier — so long as direct and indirect beneficial ownership information behind an identifier be made available to authorized users of the database — as this would allow law enforcement to track and verify the beneficial owners of covered entities more easily.

Improving Data Quality via Verification

FinCEN's draft rule rightly requires entities to submit a scanned image of an identifying document, such as a passport or driver's license, of an entity's beneficial owner(s). The decision to require a digital copy of the document will help ensure that information in the database is "accurate, complete, and highly useful" for law enforcement and authorized users. The image can be used to corroborate the identity of the owner, verify the reported data, and could help mitigate inaccurate or fraudulent submissions of data to the directory.

---

[20] "Introducing the Legal Entity Identifier (LEI)," Global Legal Entity Identifier Foundation, https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei (accessed January 5, 2022).
[21] "LEI Statistics," Global Legal Entity Identifier Foundation, last modified February 1, 2022, https://www.gleif.org/en/lei-data/global-lei-index/lei-statistics.
[22] Government Accountability Office, *Government is Analyzing Alternatives for Contractor Identification Numbers*, GAO-12-715R (June 12, 2012), 9-10, https://www.gao.gov/assets/gao-12-715r.pdf.
[23] National Defense Authorization Act for Fiscal Year 2021, § 6401(7)(A) [see note 3].

To help ensure the accuracy and completeness of the data as it is entered into the database, FinCEN should undertake additional verification measures. Much like in the private sector, such as when a credit card company declines a consumer's transaction because it does not match the company's internal files, entities registering for a FinCEN number should be notified immediately if they input incorrect information. This could save small businesses the effort of having to resubmit forms due to a typo weeks or even months after they initially register. Such verification mechanisms would be a commonsense practice that would encourage swift and comprehensive compliance with beneficial ownership information requirements, saving reporting companies time and money. These measures also ensure the accuracy and completeness of the data as it is submitted to the database, increasing the likelihood that this data is highly useful to law enforcement officers and other authorized users.

Conclusion

The Corporate Transparency Act was a significant victory for the financial transparency community. It requires FinCEN to establish a beneficial ownership database that will enable law enforcement and bank officials to identify the true owner of companies operating in the U.S., protect the integrity of the U.S. financial system, and expose shell companies engaging in illicit financial activities that undermine U.S. national security and foreign policy interests. The database will cut through the layers of anonymity often built into financial transactions, and protect U.S. taxpayer dollars by helping investigators identify and prevent fraud in U.S. public contracting.

In order to make this database as "accurate, complete, and highly useful" as possible, FinCEN should retain this rule's faithful definition of a reporting company, retain this rule's strong definition of a beneficial owner (absent the language surrounding senior officers), retain this rule's timely reporting requirements, and retain this rule's efforts to minimize cost of compliance for covered entities. FinCEN should also clarify the exemption for subsidiaries of reporting companies (exemption 22), require mandatory LEI numbers, and impose additional verification mechanisms in order to strengthen this rule and improve the accuracy and usefulness of reported information.

Thank you for your consideration of this comment. Should you have any questions, please contact me at joanna.derman@pogo.org.

Sincerely,

Joanna Derman
Policy Analyst

THE SENTRY
WAR CRIMES SHOULDN'T PAY

Statement for the Record by The Sentry

House Financial Services Committee

"Oversight of the Financial Crimes Enforcement Network"

April 28, 2022

The Sentry is pleased to submit this Statement for the Record to support of the work of the Financial Crimes Enforcement Network (FinCEN), to urge swift and strong implementation of the Corporate Transparency Act and other critical rulemakings, including on the real estate sector. We also request necessary funding for the agency to manage its increasing workload, now only magnified by the need to target Russian oligarchs and their gatekeepers and enablers in response to the war in Ukraine.

FinCEN's Critical Role

The Sentry is an investigative and policy organization that seeks to disable multinational predatory networks that benefit from violent conflict, repression, and kleptocracy. Launched in 2016, The Sentry produces hard-hitting investigative reports and dossiers on individuals and entities connected to grand corruption and violence. We advocate for the use of tools of financial and legal pressure, including anti-money laundering and illicit finance measures, targeted network sanctions, criminal prosecutions, compliance actions by banks and other private companies, and asset recovery. As a result of our work, money laundering routes have been exposed and shut down, assets have been frozen, travel has been banned, and corrupt networks have been cut off from the international financial system.

One of the principal agencies The Sentry collaborates with to achieve these objectives is FinCEN. Since The Sentry's launch, we have worked closely with FinCEN leadership and staff to take action against the money laundering that underlies violent kleptocracies, particularly in East and Central Africa. In 2017 and 2018, FinCEN issued important Advisories on illicit finance in South Sudan and on the connection between serious human rights abuse and corruption, which helped to elevate the risk profile of these concerns for the banking community. More recently, FinCEN released an Advisory focused on the risks from kleptocracies, highlighting Russia in particular.

FinCEN plays a crucial role in protecting the American economy from the threat of money laundering and illicit finance, from both domestic and foreign sources. From the current threats posed by the Russian government and network of oligarchs (some of whose wealth comes via exploitation of natural resources in sub-Saharan Africa) and their gatekeepers to regimes such as Iran and Venezuela to more general concerns such as money laundering through real estate and cryptocurrency, FinCEN's mandate and scope is uniquely local and international at the same time, given that the US financial system is itself at once both local and international.

In the years ahead, FinCEN's role will only grow more important to the ability of US regulatory and law enforcement to catch up with and even get ahead of the array of risks the financial system faces. FinCEN plays a central role in implementing the US strategy on countering corruption, as well as several critical new proposed rules and initiatives, and in tracking new and emerging threats, including the impact of the ongoing crisis in Russia and Ukraine.

Strong CTA Implementation

At the top of the list of FinCEN's priorities is implementation of the Anti-Money Laundering Act and the Corporate Transparency Act (CTA)—landmark pieces of legislation. If robustly implemented, the provisions of both laws will be cornerstones in FinCEN's ability to address current and emerging risks.

The CTA in particular needs swift and strong attention. In February, The Sentry was pleased to lead a coalition of 23 human rights organizations from around the globe in urging implementation of the initial proposed rule focused on the CTA's required establishment of a corporate registry of beneficial owners. This registry will help bring transparency and accountability to human rights abusers who have been benefiting financially from their malign activities, and it will begin to address the problem of anonymous corporate ownership that has been widely reported, most recently in the blockbuster "Pandora Papers" series that firmly pointed the finger at US financial secrecy.

FinCEN is unfortunately behind in its rulemaking and implementation efforts. Congress should maintain strong oversight to ensure that the agency completes all work to finalize CTA rulemakings by December 1, 2022. Given that implementation of the CTA is also a priority related to the Summit for Democracy and that the United States will serve as host to the next International Anti-Corruption Conference, FinCEN's delivery of final products for these events in December would prove US commitment and provide encouragement to other countries.

FinCEN's initial proposed rule on beneficial ownership reporting requirements is a meaningful and faithful interpretation of the statute and congressional intent. Nevertheless, oversight will help maintain this course and ensure that competing interests are not able to roll back this opportunity. As noted in our letter with other human rights organizations, The Sentry urges FinCEN to ensure that the rule appropriately tailors the scope of certain exemptions, maintains its coverage of certain forms of trusts used to exploit the real estate market, and collects from reporting entities actionable information—such as the residential addresses of beneficial owners—so that information can be connected to real people.

Looking ahead to future rulemakings on the CTA, we urge Congress to encourage FinCEN to make the eventual corporate database easy to use, including by adhering to the Open Ownership principles. FinCEN should maintain simple and uncomplicated protocols for access by law enforcement and other users, while also facilitating information sharing with trusted foreign law enforcement agencies that may need the underlying information for multi-jurisdiction investigations.

Addressing Money Laundering in Real Estate

A recent study by Global Financial Integrity found that at least $2.3 billion has been laundered through the U.S. real estate market in the past five years. In November 2021 as part of a massive reporting project connected to a leak of banking documents, The Sentry reported on money laundering scandals involving Congolese officials moving illicitly obtained funds into the US real estate market, including in Rockville, MD—Congress' backyard—and receiving tens of millions of dollars in bribery payments related to massive mining and infrastructure deals from Chinese companies and middlemen. These are just two of the myriad money laundering schemes routing through the US financial system from networks like those of former Congolese President Joseph Kabila. Such schemes threaten not only the potential for peace and good governance in foreign countries, but also the integrity and soundness of the US economy.

Though the Treasury Department and national security officials identified the US real estate market as a money laundering vulnerability more than 20 years ago, real estate professionals have had a "temporary exemption" from having to fulfill anti-money laundering obligations similar to those required of other financial institutions, thereby offering a gateway to the US financial system. In December, FinCEN initiated a rulemaking to update US anti-money laundering safeguards for the US real estate sector.

Congress should encourage FinCEN to deliver a timely proposed rule instituting safeguards for the US real estate sector by December 2022, as another demonstration of US commitment to combat corruption and illicit finance.

FinCEN Funding and Staffing

To achieve the priorities noted above, FinCEN needs additional funding and staff. The administration requested $210 million for FinCEN for FY23. That should be seen as the floor for Congress, not the ceiling. In FY22, Congress underfunded the administration's request by $30 million. This should not be repeated, and Congress should consider delivering the additional funds that were lacking in FY22.

To implement the CTA, tackle money laundering in real estate, track Russian oligarchs' assets and target their enablers, as well as continue to deliver on the agency's baseline priorities, FinCEN requires high-level and trained professionals to keep up with both the financial institutions the agency partners with and the criminal networks they seek to disrupt and penalize. As the "FinCEN Files" showed in 2020, in many potential money laundering investigations, banks are fulfilling their end of the bargain by submitting the Suspicious Activity Reports required of them; the issue is that FinCEN lacks the staff and resources to follow up on these leads.

Conclusion

FinCEN serves a crucial function to uphold US national security and, by extension, to protect human rights. This has been made ever clearer by the conflict in Ukraine, and we encourage FinCEN to focus on tracking the assets of Russian oligarchs and target their gatekeepers as it strengthens work

on its existing priorities. The Sentry asks Congress to support FinCEN by providing clear guidance on the implementation of legislative actions and by financing the staffing and other resources needed to deliver critical data for law enforcement investigations and advance much-needed reforms to safeguard the US financial system.

DEMOCRATS ABROAD

April 20, 2022

The Honorable Maxine Waters
Chairwoman - House Financial Services Committee
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member - House Financial Services Committee
United States House of Representatives
4340 O'Neill House Office Building
Washington, D.C. 20024

Re: Hearing on Oversight of the Financial Crimes Enforcement Network on April 28, 2022

Dear Chairwoman Waters, Ranking Member McHenry, and Members of the Committee:

Democrats Abroad greatly appreciates your holding this important hearing. We recognize the importance of the Financial Crimes Enforcement Network's mission to combat money laundering and terrorist financing. Today we are submitting policy proposals based on the firsthand experiences of our 200,000 members.

Since the passage of the Currency and Foreign Transactions Reporting Act (more commonly known as the Bank Secrecy Act) in 1970, U.S. citizens living abroad ("non-residents") have increasingly become caught up in ongoing efforts against tax evasion and malicious actors. While we recognize that battling moneylaundering and terrorist financing are critical priorities, substantial adjustments to FinCEN Form 114, the Report of Foreign Bank and Financial Accounts or "FBAR," are needed to ensure that the impact to ordinary law-abiding citizens is proportional to the financial law enforcement benefits.

The FBAR is a duplicative, burdensome and confusing information report, which no longer serves a meaningful purpose given the availability to the Treasury Department of similar information from multiple other sources. **FBAR information collection from U.S. citizens who reside outside the United States is an undue burden** for the following reasons:

- Awareness of the FBAR filing requirement is low among ordinary middle class citizens who reside outside the United States. Filing follows a

Democrats Abroad
PO Box 15130
Washington, DC 20003
(202) 733-6790

multi-step online process which is completely separate from tax return preparation and filing, and many professional tax preparers do not routinely ask questions that would identify whether an individual has a filing requirement.

- The filing requirements and definitions are difficult to understand. For an ordinary individual reading the instructions provided with the form, it is difficult to determine whether reporting of certain account types (such as non-U.S. pensions, prepaid transit cards, or cashless payment apps) is required or not. Professional tax preparers are often hesitant to offer advice on these questions, other than to say that conservatism is prudent given the extraordinarily high penalties for compliance failures, even if non-willful.
- Filing thresholds have not been revised in almost 50 years and are inordinately low. Once an individual has triggered the filing requirement as a result of having aggregate financial assets greater than $10,000, then all non-U.S. financial accounts must be declared, with no de minimis exemption. For instance, even dormant accounts with zero balance must be reported.
- The fact that penalties are assessed on a per-account, not a per-form, basis and the fact that the per-account penalty often exceeds the balance of the account means that accidental non-compliance comes with terrifying consequences.
- FBAR filings are largely duplicative with the information collected on other IRS forms such as Form 8938 ("Statement of Foreign Financial Assets"), Form 8621 ("Information Return by a Shareholder of a Passive Foreign Investment Company or Qualified Electing Fund") and Form 3520A ("Annual Information Return of Foreign Trust with a U.S. Owner"). In addition to the duplicative information reporting required of individuals, FATCA requires Foreign Financial Institutions to file Form 8966 disclosing balances and income associated with accounts owned by U.S. citizens.
- Finally, FBAR's requirement for information on accounts for which the U.S. citizen does not have a beneficial interest but only signature authority is also a major cause of misunderstanding and unintentional compliance failures. It also leads overseas corporations to remove U.S. citizens from positions of authority over financial matters, limiting the career opportunities for those impacted.

If all of the 9 million U.S. citizens who reside outside the United States actually complied fully with the FBAR filing requirements, FinCEN would be inundated with an overload of useless information about the everyday financial activities of ordinary people. This would not support FinCEN's mission of combating money laundering, but rather drown out actual indicia of risk in a tidal wave of unnecessary information.

Democrats Abroad
PO Box 15130
Washington, DC 20003
(202) 733-6790

The GAO has called attention to the overlap and redundancy of information being fed to Treasury and called for consolidation and simplification to relieve the burden on Americans abroad[1]. In addition, the "challenges" identified by the GAO in 2018 with "...complying with US tax reporting requirements on their foreign retirement savings"[2] can be very onerous, often requiring expensive professional assistance, which further induces fear of punitive sanctions and stresses caused by forcing unwilling non-US spouses and business associates into US reporting further discourage compliance.

Without evidence of serving any purpose for combatting moneylaundering and terrorist financing activities, **administering the FBAR regime is consuming resources which could be deployed to other activities, and has not shown the practical utility that is required to justify its continuation**.

Our recommendations are intended to help FinCEN achieve proportionality while simultaneously improving FBAR's effectiveness as a law enforcement tool.

Policy Recommendations:

- A one-time **adjustment of FBAR reporting thresholds** to $70,000, which accounts for inflation in the 50 years since FBAR's introduction, followed by annual inflation adjustments thereafter.
- **Thresholds should be customized to take into account "Geographic Risk."** The motivations and justifications for holding non-US accounts differ greatly between resident and non-resident US citizens. Specifically, either:
    - An exemption of non-residents from reporting OR
    - A significantly higher reporting threshold for non-residents on the order of $400,000 (consistent with IRS Form 8938)
- Given Form 8966 reporting by financial institutions, it is not clear why individual filings are required at all. At a minimum, **the two individual bank account filing requirements (FBAR and Form 8938) should be consolidated and shared between IRS and FinCEN as necessary**.

[1] Foreign Asset Reporting, Actions Needed to Enhance Compliance Efforts, Eliminate Overlapping Requirements, and Mitigate Burdens on U.S. Persona Abroad, [GAO-19-180], April 2019

[2] Workplace Retirement Accounts: Better Guidance and Information Could help Plan Participants at Home and Abroad Manage Their Retirement Savings, [GAO-18-19], January 2018, "Highlights"

Democrats Abroad
PO Box 15130
Washington, DC 20003
(202) 733-6790

Please note that this has been a recurring point of feedback from the IRS National Taxpayer Advocate for multiple years.[3] [4] [5] [6]

- **Improving the proportionality of enforcement/penalties for FBAR violations and clearly defining willful vs. non-willful recommendations**. We note that this has also been a point of feedback from the IRS National Taxpayer Advocate.[7]
- Restoration of paper FBAR filings and improvement of e-Filing options to allow popular tax-filing software to include FBAR e-filing.
- **Exclusion of accounts under a de minimis threshold**, even when the reporting obligations are triggered based on aggregate foreign bank account balances.
- For non-residents, exclusion of accounts where a US Person only has signatory authority on the account but in which they have no beneficial interest.

At the present, **FBAR reporting is redundant, disproportionate to risk, and it fails to take into account the necessities of holding foreign bank accounts when residing outside of the United States. At the same time, enforcement efforts are generally disproportionate**, with FinCEN exercising little discretion and often pursuing statutory-maximum penalties even for infractions deemed non-willful. This results in highly, highly, regressive penalties that disproportionately harm the middle and working class. In some cases, fear of excessive penalties is cited as a barrier to becoming compliant for previous non-filers.

Our proposals for reform are intended to reduce paperwork burdens for both the public and FinCEN, align reporting to accounts that are large enough to pose a substantial risk relating to financial crimes, and to ensure that enforcement serves a public benefit.

We thank you for the opportunity to provide commentary and recommendations, and we encourage you to read our responses to specific questions in the annex included with our letter.

---

[3] https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2022/01/ARC21_PurpleBook_02_ImproveFiling_8.pdf

[4] https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2021/01/ARC20_PurpleBook_02_ImproveFiling_9.pdf

[5] https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2020/08/ARC19_PurpleBook_02_ImproveFiling_8.pdf

[6] https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2020/07/ARC18_PurpleBook.pdf, Recommendation #12

[7] https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2021/01/ARC20_PurpleBook_04_ReformPenInts_35.pdf

Democrats Abroad
PO Box 1513C
Washington, DC 20003
(202) 733-679C

Thank you for the opportunity to provide this testimony.

Please do not hesitate to contact Rebecca Lammers of our Taxation Task Force on taxadvocacy@democratsabroad.org with any questions about the information and recommendations provided.

Sincerely,

Candice Kerestan
International Chair
Democrats Abroad
chair@democratsabroad.org

Rebecca Lammers
Chair, Taxation Task Force
Democrats Abroad
taxadvocacy@democratsabroad.org

cc:

The Honorable Nancy Pelosi
Speaker of the House
US House of Representatives
Office of the Speaker, United States Capitol
Washington, DC 20515

The Honorable Kevin McCarthy
Republican Leader
U.S. House of Representatives
H-204, United States Capitol
Washington, DC 20515

The Honorable Charles Schumer
Majority Leader
United States Senate
S-224, United States Capitol
Washington, DC 20515

The Honorable Mitch McConnell
Republican Leader
United States Senate
S-230, United States Capitol
Washington, DC 20515

The Honorable Richard E. Neal
Chairman - Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, DC 20515

The Honorable Kevin Brady
Ranking Member - Committee on Ways and Means
U.S. House of Representatives
1139 Longworth House Office Building
Washington, DC 20515

The Honorable Ron Wyden
Chairman - Committee of Finance
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member - Senate Finance Committee
United States Senate
219 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Carolyn Maloney
Americans Abroad Caucus
3408 Rayburn House Office Building
Washington, DC 20515

The Honorable Maria Salazar
Americans Abroad Caucus
1616 Longworth House Office Building
Washington, DC 20515

The Honorable Dina Titus
Americans Abroad Caucus
2464 Rayburn House Office Building
Washington, DC 20515

Democrats Abroad
PO Box 15130
Washington, DC 20003
(202) 733-6790

April 28, 2022

The Honorable Maxine Waters
Chair
Committee on Financial Services
U.S. House of Representatives
Washington, DC, 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC, 20515

Dear Chair Waters, Ranking Member McHenry, and Members of the Committee,

My name is Nicholas Anthony. I am a policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives. I appreciate the opportunity to provide input to assist the committee with its hearing titled, "Oversight of the Financial Crimes Enforcement Network."[1] The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets, and peace, and the Center for Monetary and Financial Alternatives focuses on identifying, studying, and promoting alternatives to centralized, bureaucratic, and discretionary monetary and financial regulatory systems. The opinions I express here are my own.

Measuring Effectiveness and Accountability

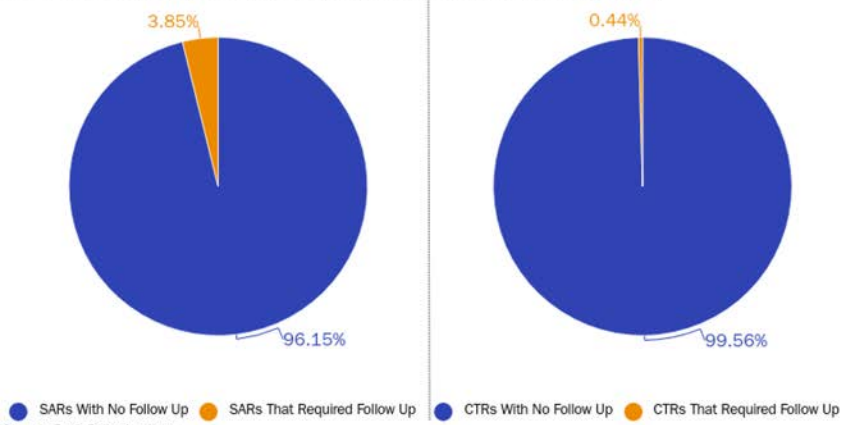
The Financial Crimes Enforcement Network (FinCEN) is charged with combatting financial crimes like money laundering and terrorist financing. In practice, that has resulted in FinCEN becoming a depository of financial information on Americans both large and small. FinCEN reported that it received more than 20 million Bank Secrecy Act (BSA) reports in 2019 alone.[2] And it is estimated that complying with the BSA in 2019 cost the U.S. financial industry $31.5 billion—up from an estimated $4.8 billion to $8 billion in 2016.[3] However, what is not known is what was done with those 20 million reports. FinCEN referred to the reports as providing "potentially useful information to agencies whose mission is to detect and prevent [financial crimes]," but it did not say if those reports were *in fact* useful to that mission.[4]

[1] U.S. House Committee on Financial Services, "Oversight of the Financial Crimes Enforcement Network," Full Committee Hearing, April 28, 2022, https://financialservices.house.gov/events/eventsingle.aspx?EventID=409259.
[2] Financial Crimes Enforcement Network, "What is the BSA Data?," https://www.fincen.gov/what-bsa-data.
[3] LexisNexis Risk Solutions, "True Cost of AML Compliance Study," 2019, https://risk.lexisnexis.com/insights-resources/research/2019-true-cost-of-aml-compliance-study-for-united-states-and-canada; Norbert Michel and David Burton, "Financial Privacy in a Free Society," Heritage Foundation, September 23, 2016, https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society.
[4] Financial Crimes Enforcement Network, "What is the BSA Data?," https://www.fincen.gov/what-bsa-data.

A 2018 study from the Bank Policy Institute (BPI) provides strong evidence that those reports were not useful.[5] After surveying a sample of 19 financial institutions, BPI found that a median of 4% of suspicious activity reports (SARs) and an average of 0.44% of currency transaction reports (CTRs) required additional review from law enforcement (Figure 1). Even fewer reports likely resulted in stopping or apprehending criminals.

Figure 1

Effectiveness of suspicious activity reports (SARs) and currency transaction reports (CTRs)



Source: Bank Policy Institute

It's time for FinCEN to begin reporting on its own activity.[6] FinCEN should annually report, at the least, how many SARs and CTRs:

1. Required a desk rejection
2. Required secondary review
3. Led to law enforcement action
4. Led to a unique criminal conviction
5. Led to a criminal conviction in conjunction with an existing investigation

[5] Bank Policy Institute, "Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance," October 29, 2018, https://bpi.com/wp-content/uploads/2018/10/BPI-AML-Sanctions-Study-vF.pdf.

[6] For additional recommendations, see Norbert Michel and Nicholas Anthony, "Review of Bank Secrecy Act Regulations and Guidance," February 7, 2022, https://www.cato.org/public-comments/review-bank-secrecy-act-regulations-guidance.

While more information would be preferable, these surface-level statistics could greatly improve how Congress and the public evaluate the effectiveness of FinCEN and the anti-money laundering (AML) regime at large. Americans deserve to know how the government justifies enforcing this regulatory framework, but their elected representatives cannot properly judge the effectiveness of FinCEN without more information.

Respectfully,

Nicholas Anthony
Policy Analyst
Center for Monetary and Financial Alternatives
The Cato Institute

MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
Washington, DC 20515

PATRICK McHENRY, NC
RANKING MEMBER

March 2, 2022

The Honorable Janet Yellen
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C, 20220

Mr. Himamauli Das
Acting Director
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, Virginia 22183

Re: Department of the Treasury's Notice of Proposed Rulemaking Titled "Beneficial Ownership Information Reporting Requirements," RIN 1506-AB49, FINCEN -2021-0005, 86 Fed. Reg. 69920 (December 8, 2021)

Dear Secretary Yellen and Acting Director Das:

We write to express our serious concern with the Department of the Treasury's Notice of Proposed Rulemaking titled "Beneficial Ownership Information Reporting Requirements" (NPRM), released on December 8, 2021. The NPRM in its current form is too complex, overly broad, and deviates significantly in many ways from Congress' intent as it relates to the new beneficial ownership information reporting regime. Moreover, we are concerned that if the issues raised in this letter and by the hundreds of interested parties are not addressed, the final rule will not only harm legitimate small businesses but will undoubtedly create additional loopholes for bad actors to exploit.

Congress made clear its agreed-upon framework for reporting and collecting beneficial ownership information in Division F of the National Defense Authorization Act, Fiscal Year 2021. This statutory framework is intended to accomplish three objectives. The first is to stop bad actors from using "shell companies" to exploit the financial system to conduct terrorism or other illicit activities. In addition, the framework is intended to minimize any new burdens the new regime will have on reporting companies, particularly smaller companies. Finally, the statutory framework is intended to provide clear rules of the road for reporting companies regarding their beneficial ownership responsibilities.

Disconcertingly, the NPRM deviates from this statutory framework in several, significant ways. First, the NPRM is too complex and overly broad. Understanding the NPRM in its current form will take hours for many small reporting companies to understand. As a result, these entities will more likely than not require the help of an attorney, CPA, or other individual(s) to navigate their reporting obligation. For example, the NPRM's:

- Interpretation of substantial control is inconsistent with other federal statutes, confusing, and overly broad. As you know, Treasury already has significant experience determining "control" pursuant to Section 721 of the Defense Production Act (DPA). The DPA defines the term as "the power, direct or indirect, whether exercised or not exercised, to determine, direct, or decide important matters affecting an entity." This definition itself was derived from longstanding Treasury regulations. The term "substantial control" is only coherent as a narrower subcategory of "control," particularly a form of control that is ultimate in nature and is tied to benefits enjoyed by a beneficial owner.

  In addition, prior to enactment of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), controlling investments under the DPA did not necessarily encompass board membership or substantial influence ("substantive decision-making," per the amended DPA), requiring such contingencies – as Treasury itself advocated at the time – to be covered as examples of *non-control* under a new Section 721(a)(4)(D). Board membership and substantial influence are therefore not concepts that need to entail control at all, and they are certainly not identical to the narrower "substantial control." Having drafted FIRRMA, the Committee on Financial Services was aware of these important distinctions when drafting the framework.

  Finally, the proposed listing of senior officers of a reporting company is nonsensical. Such persons, in the absence of substantial ownership rights, violate any commonsense dictionary definition of the term "beneficial owner." Anyone with familiarity with the debate surrounding the new beneficial ownership information reporting regime will show that the statutory framework targeted beneficial ownership, not employment data.

- Definition of ownership or control of ownership is overly broad. Where appropriate, Congress intended those provisions of the current CDD be retained. The definition of ownership or control of ownership is one of the provisions that should be retained.

- Definition of company applicants is overly broad. Congress did not intend to capture an entire law firm or company in the simple filing of corporate documents.

- Requirement that reporting companies provide digital photographs of beneficial owners deviates from the statutory framework. Congress did not intend for reporting companies, particularly those with fewer than 20 employees, to submit digital photographs of their beneficial owners.

- Requirement of residential addresses is inconsistent with the statutory framework. Congress intended to give reporting companies a choice between filing a beneficial owners' business address or residential address. It was not intended to limit addresses to residential only.

- Definition of a reporting company is overly vague and inconsistent with the statutory framework. Congress did not explicitly include general partnerships, sole-proprietorships or trusts in the definition of reporting companies because it did not intend for them to be

included. The decision to include them, sua sponte, is another example of overreach that if left unaddressed will negatively impact tens of millions of small businesses.

- Suggested submission of TIN, DUNES, or LEI numbers is inconsistent with the statutory framework. Congress did not intend for any reporting company to submit this type of information even if voluntary. Congress was clear on the four pieces of beneficial ownership information that it intended reporting companies to submit: legal name; date of birth; current residential or business street address; and unique identification number from an acceptable identification document (i.e., driver's license or passport).

- Reporting rules for exempt entities is inconsistent with the statutory framework. Congress did not intend for any exempt entity to report to Treasury. Thus, the requirement that companies are required to submit notice to FinCEN that they are exempt from compliance deviates from the statutory framework.

- Discussion on when a FinCEN Identifier should be used is nonsensical. Simply stated Congress intended the Identifier to be a tool available to reporting companies to simplify their filings. The insinuation that reporting companies will use the Identifier for nefarious purposes, without any type of evidence, is concerning and should be removed immediately.

Notwithstanding the above concerns, the NPRM deviates significantly from the statutory deadlines for reporting information, updating information, and correcting inaccurate information. Congress was unambiguous that the timeframe for current reporting companies to provide the four pieces of beneficial ownership information was two years from the effective date of the reporting regulation. Moreover, Congress did not intend for new reporting companies to file within 14 days. A more reasonable timeframe for a new reporting company to file beneficial ownership information is 90 days from the time the entity files state organic documents. In addition, the 90-day time period should be applied to those companies that may no longer be exempt from filing beneficial ownership information.

Congress was also unambiguous that reporting companies providing updated information would have a year to provide this information. Moreover, Congress was very specific that any change to this deadline was contingent on the Department of Treasury, in consultation with the Department of Justice and the Department of Homeland Security, conducting a review of evidence demonstrating a legitimate need to shorten this time frame. Given that the new regulation is not even in effect and the Department of Treasury has no evidence demonstrating the need for a shorter time period, the statutory time period for updating information must remain one year.

The issues raised above only touch the surface. Yet, together with the concerns expressed by the hundreds of interested parties, deepen our concern about the Department's underlying motivation for the new beneficial ownership information reporting regime. Let us be clear, previous partisan attempts to reform the beneficial ownership reporting regime were rejected by Congress. In fact, proposals to: (1) establish an open and vast collection regime, like that established in the United Kingdom; (2) impose numerous and costly reporting requirements on small businesses; (3)

jeopardize the privacy and security of small businesses' personal identifiable information; and (4) enable small businesses' PII to be accessed with few limitations, were met with fierce resistance.

Adherence to the statutory framework set out in Division F of the NDAA is critical. The United States is not the United Kingdom. Legitimate small businesses in this country have the most to lose in this new reporting and collection regime. Small businesses historically operate on thin margins. The global health crisis over the last two years have only exacerbated these margins. Additional burdens will impact the approximately 25 million existing reporting companies and the 3 million new reporting companies formed each year (according to FinCEN's own estimates). In fact, according to FinCEN's own initial regulatory flexibility analysis (IRFA), the current NPRM will have a significant economic impact on small companies. FinCEN estimates there will be 32,800,422 burden hours in the first year and 9,468,510 burden hours each year thereafter. The total costs for this rule once in effect is expected to total $1.26 billion in the first year and $364 million thereafter. It is unacceptable to acknowledge and recognize, as you do in the NPRM, the impact on small businesses, and fail to draft a rule that adheres to congressional intent by minimizing the burdens on them.

Given these potential costs, the Department of Treasury must ensure that any new reporting burdens on small businesses are minimal. This includes rescinding the current Customer Due Diligence Rule set forth in 31 CFR 1010.230 (b)-(j) immediately upon the effective date of this NPRM. We are disconcerted by references to the rescission being addressed in subsequent rulemaking. Congress intended these provisions to be rescinded immediately upon the effective date of this regulation not years after the fact. This is to ensure that there is one clear rule that sets out the responsibilities of reporting companies – not multiple reporting regimes. This error must be addressed immediately.

We are optimistic you understand the magnitude of our concern. The statutory framework reflects bipartisan consensus that the Department of the Treasury stay within the four corners of the statute, obtain evidence, and build out a new reporting and collection regime based on direct evidence rather than anecdotes that create more loopholes for bad actors to exploit at the expense of legitimate businesses. We urge you to go back to the statutory framework and revise the NPRM accordingly. We look forward to working with you to establish a beneficial ownership information reporting regime that Congress intended.

Sincerely,

Patrick McHenry
Ranking Member
House Committee on
Financial Services

Blaine Luetkemeyer
Ranking Member
House Committee on
Small Business

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

April 27, 2022

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing: "Oversight of the Financial Crimes Enforcement Network"

Dear Chairwoman Waters and Ranking Member McHenry:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to share our thoughts on issues of importance to credit unions ahead of tomorrow's hearing entitled "Oversight of the Financial Crimes Enforcement Network." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 130 million consumers with personal and small business financial service products. We would like to thank you for holding this important hearing and the opportunity to provide input from credit unions as it relates to the Financial Crimes Enforcement Network (FinCEN).

NAFCU has repeatedly requested the modernization and streamlining of suspicious activity reports (SARs), including increasing the reporting thresholds, streamlining the SAR form to remove redundant and obsolete provisions, and providing a simplified SAR form for continuous filings. Modernizing and increasing the required reporting thresholds is the highest priority of NAFCU members in producing reports and records that are highly useful in countering financial crime. NAFCU encourages FinCEN to tie the reporting thresholds to inflation and increase them in order to decrease the burden on credit unions. The SAR reporting thresholds have remained unchanged for decades even though inflation is occurring at a rapid rate. To address this, NAFCU recommends that FinCEN immediately begin studying the impacts of tying the SAR reporting thresholds to inflation. The outdated thresholds cause some SARs to be useless to law enforcement because behavior that was once thought of as suspicious has since become common transaction practice. We also urge Congress to consider action to modernize the thresholds.

As you know, Section 6403 of the *Corporate Transparency Act* (CTA) requires reporting companies to provide beneficial ownership information to FinCEN, which must maintain the information in a secure, non-public database. Members routinely rely on their credit unions to assist with all financial matters, and as their trusted financial partner, credit unions will likely help in explaining beneficial ownership reporting requirements. However, under no circumstances should any burden of notifying reporting companies of any obligation fall on credit unions. Respondents to NAFCU's 2021 Federal Reserve Meeting Survey reported that their *Bank Secrecy Act*/Anti-Money Laundering (BSA/AML) regulatory burden has increased by more than 68 percent in the past five years, and they expect that increase to

reach over 79 percent in the next five years. Imposing even greater BSA/AML-related regulatory burdens on community financial institutions through additional obligations to ensure companies are reporting beneficial ownership information to FinCEN's new database would not only increase costs on already resource-strapped institutions, but also make it harder for credit unions to serve their communities by offering affordable products and services.

As cryptocurrency and digital assets become more prevalent in our financial system, they may become a target for suspicious activity and the facilitation of illicit finance. FinCEN has previously indicated that the agency views itself as "technology neutral" and regulates the activity of money transmission and not just certain types of transactions. NAFCU supports this approach and encourages FinCEN to maintain this viewpoint. As FinCEN and other federal agencies work together on an initial government-wide strategy regarding digital assets regulation and supervision, it is important that FinCEN maintain its technology neutral stance. Credit unions continue to abide by BSA/AML regulations and rules as their members begin to conduct transactions with exchanges and purchase digital assets and are experiencing an increasing number of wire transfer and Automated Clearing House (ACH) transactions. Risks associated with digital assets remain a significant concern until FinCEN provides additional transparency regarding the monitoring of these transactions. FinCEN has listed cryptocurrency as a national priority; thus, it is important that financial institutions have sufficient guidance regarding integration of this priority into their risk assessments.

We thank you for the opportunity to share our thoughts and recommendations and look forward to continuing to work with you as you conduct oversight on FinCEN. Should you have any questions or require any additional information, please contact me or Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at jrelfe@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the U.S. House Committee on Financial Services

April 28, 2022

The Honorable Maxine Waters
Chairwoman
2128 Rayburn HOB
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
4340 O'Neill HOB
Washington, DC 20515

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled "Oversight of the Financial Crimes Enforcement Network." SentiLink is a leader in identity verification technology. With real-time scoring capabilities, our models target synthetic identities – both first-party and third-party – which are often missed in basic Know Your Customer ("KYC") and Customer Identification Program ("CIP") processes, as well as identity theft. Further, our KYC Insights tool helps our partners by uncovering insights about identity risks, empowering financial institutions to make better identity decisions.

The Financial Crimes Enforcement Network ("FinCEN") plays a vital role in crafting the rules intended to combat identity crimes. Those rules, including the risk-based KYC and CIP frameworks, are out-of-date and not meeting the threats posed by the changing fraud landscape. As such, SentiLink encourages the Committee to focus on the need for modernizing the requirements around identity verification in the financial industry. In particular, we offer the following:

- CIP rules should provide greater clarity and specificity with regards to what constitutes a "reasonable belief" of identity verification, and should focus on the changing nature of the actual criminal threats financial institutions face, agnostic to the specific product or service for which a consumer is applying.
- Checks for synthetic identity fraud should be a core feature of CIP rules, FAQs and guidance.
- CIP rules should reflect the reality of the changing nature of identity fraud, and require the collection and additional verification of address, phone or e-mail, depending on the means by which an institution contacts their customers.

Existing Risk-Based KYC Rules Fuel Identity Theft and Miss Synthetic Identities

Identity theft, Checking Accounts and the Pandemic

The foundation of the CIP rules rests on the basic but critical premise that a financial institution must "form a reasonable belief that it knows the true identity of each

customer."[1] These rules have been deliberately drafted to require risk-based procedures. For example, current rules make clear that an application for a "resident consumer account" (i.e., a basic checking account) requires less identity diligence -- compared to, for example, a high net worth private banking application -- because it is a lower-risk product.[2] However, identity fraud has evolved in such a way as to make this assumption unreliable as the challenge of identifying what constitutes risk for a financial institution is no longer as obvious.

This was brought into focus during the pandemic, where fraudsters would use stolen identities to open "low-risk" checking accounts with ease in order to apply for government relief funds. When the funds were received into these checking accounts, they could be laundered through a myriad of other financial accounts. *Overall, from September, 2020, to June, 2021, the percentage of applications for demand deposit accounts identified by SentiLink as using stolen identities increased 187%.*

Missing Synthetics

Synthetic identity fraud occurs when a criminal engineers a fake person. Often this involves a true name and date-of-birth but a not-yet-issued Social Security number ("SSN"), or one issued to a minor. Another method involves a fictitious name and date-of-birth, but paired with a valid SSN.

As a typology, synthetic identity fraud has been designed to circumvent basic KYC/CIP processes. As such, it is no coincidence that basic identity verification processes fail to detect it with such regularity. For financial institutions, our analysis of the behavior of synthetic identities over time reveals the potential for increased financial losses. Looking at the credit card market, for example, our data illustrates how synthetic identities that have been built to a "prime"-level credit score tend to charge off 75% of the time within 23 months for an average loss of $13,000, compared to the performance of legitimate consumers who would be expected to charge off at a rate of 1.5% during the same time. In fact, we've found up to 10% of a credit card issuer's chargeoffs are actually due to synthetic fraud.

The Means of Communication Matters More for Identity Verification

In general, to comply with existing CIP regulations, a financial institution must obtain information on a potential customer's name, date of birth, identification number and address prior to opening an account.[3] However, reliance on a consumer's address has

[1] 31 CFR 1020.220(a)(2)
[2] See "Appendix K" in the FFIEC's BSA/AML Manual for Examiners.
[3] 31 CFR 1020.220(a)(2)(i)(A)

created a regulatory gap: Modern identity thieves regularly leverage this well-known CIP compliance formula of a legitimate person's name + date of birth + identifier + address PII combination -- but paired with a means of electronic communication controlled by the fraudster -- to successfully obtain credit. An application with a street address that ties to the applicant is no longer a reliable signal that the applicant is legitimate. Given the high rate of data breaches, simply knowing a name, date of birth, identifier and address is not sufficient to determine a person's identity.

To support this conclusion, we examined just over 92,000 checking account applications over the last year that our models indicated as likely based on stolen identities. Of those:

- Nearly 55% had a consistent address history of at least two years. Of those:
    - 68% provided known risky VoIP numbers, and 82% of the phone numbers provided had an area code with no connection to the applicant.
    - 77% included a brand-new e-mail address or one that had been created less than two months before the application date.

Conclusion

Thank you for the opportunity to provide these comments. Technological change has revolutionized the way consumers and businesses access the banking system. In many cases, these innovations have fully digitized and automated the account origination process. While this has many advantages -- such as reducing costs, increasing efficiencies, and reaching new and underserved consumers -- it has dramatically heightened the importance of strong customer identity verification procedures. We look forward to engaging with you and your colleagues to advance policy solutions that protect American consumers and businesses from identity crimes.

Sincerely,

/s/

Jason Kratovil
Head of Public Policy

House Committee on Financial Services
Questions for the Record
"Oversight of the Financial Crimes Enforcement Network"
April 28, 2022

Ranking Member Patrick McHenry

1. During our recent hearing, several of my colleagues asked for updates on the implementation of the Corporate Transparency Act and its beneficial ownership reporting requirements. However, my concern is that the reporting provisions under the proposed rules are overly broad and will unnecessarily burden FinCEN by inadvertently imposing those requirements upon certain large non-public companies with publicly held non-U.S. parents. By requiring large, legitimate companies with complex corporate structures to meet the proposed reporting requirements, it will needlessly impose significant costs and burdens upon the companies and FinCEN.

   Under the proposed rule promulgated by FinCEN [Docket Number FINCEN 2021-0005 and RIN 1506-AB49], some of these companies might be exempt from reporting under the Large Operating Company exemption, which exempts company structures that have more than $5,000,000 in consolidated revenue and 20 or more employees at the taxpayer. However, others legitimately operating may not satisfy this exemption because the taxpayer does not have 20 or more employees, despite its operating subsidiaries having thousands of employees.

   a. Can you explain why the revenue amount is allowed to be aggregated but the employee threshold is not?

   Answer: In FinCEN's view, the statutory language of the Corporate Transparency Act (CTA) permits the former, but not the latter. The CTA exempts a large operating company that employs more than 20 employees on a full-time basis, filed income tax returns demonstrating more than $5,000,000 in aggregate gross receipts or sales, and has an operating presence at a physical office within the United States. For purposes of the second requirement only, the CTA specifies that the aggregate gross receipts or sales include the receipts or sales of "other entities owned by the entity" and "other entities through which the entity operates." The CTA contains no similar specification for employee headcount. To the contrary, it provides that the exception applies to an "entity that . . . employs" more than 20 employees, indicating that the determination of the number of employees is to be made on an entity-by-entity basis.

   b. Has FinCEN evaluated whether to broaden the public company exemption to include U.S. subsidiaries of public companies that are traded on European or Japanese markets?

   Answer: The final beneficial ownership information (BOI) reporting rule, published on September 30, 2022, does not include any exemptions beyond the twenty-three exemptions specifically set out in the CTA. The CTA sets a high bar for creating

additional exemptions given the concern that exemptions could create loopholes that illicit actors could exploit to evade reporting requirements: the Secretary of the Treasury, the Attorney General, and the Secretary of Homeland Security must all agree that requiring BOI from such entities would neither serve the public interest nor help further key government objectives.

In the final BOI reporting rule, FinCEN considered all comments on the BOI reporting Notice of Proposed Rulemaking, including those that suggested creating additional exemptions from the definition of "reporting company."

FinCEN will continue to consider proposals and suggestions for potential exemptions consistent with the statutory requirements.

c. Finally, the CTA authorizes the Secretary of the Treasury to prescribe regulations that "minimize the burdens on reporting companies…including by eliminating duplicative requirements" and ensure that reporting is "highly useful" to FinCEN. Acting Director Das, what is FinCEN doing to minimize the burdensome reporting requirements, and will you consider using the broad authority given to the Treasury department to better target the reporting rules?

Answer: FinCEN is mindful of the burden the rule will place on small businesses and has worked in its final BOI reporting rule to minimize burdens on reporting companies while fulfilling Congress's mandate to create a BOI database that is highly useful to national security, intelligence, law enforcement agencies, and Federal functional regulators. For instance, in response to comments on the proposed rule, FinCEN eliminated the requirement that reporting companies created or registered before the effective date provide information on company applicants. Further, reporting companies required to report company applicant information under the final rule will not have to update information about their company applicants. FinCEN will continue to seek to minimize burdens as it moves forward with CTA implementation.

FinCEN has also made a firm commitment to providing outreach and guidance materials that will make it easier for reporting companies, and small businesses in particular, to comply with this new requirement.

Representative Sylvia Garcia

1. Chairwoman, thank you for holding this hearing and thank you Director Das for being here today. One issue I've worked closely on, with my colleague on this committee, Rep. Wagner, is preventing and eliminating the spread of child sexual abuse materials (CSAM). We actually have introduced a bill together on the issue, the EARN It Act. Director Das, I am increasingly concerned of the amount of child sexual abuse material (CSAM) and sex trafficking occurring on various sexual solicitation platforms which are transacted through the US financial services sector, including Mastercard and Visa.

   While I applaud FinCEN including guidance to combat human trafficking in the Anti-

Money Laundering and Countering the Financing of Terrorism National Priorities published last year, the agency must do more through its authority and jurisdiction over the credit card operators to protect children. A recent report by the Anti-Human Trafficking Intelligence Initiative indicates a disturbingly widespread likelihood of CSAM and sex trafficking occurring on these sites. The study uses open-source methodologies that are public and easy to find showing strong linkages between these sexual solicitation sites and this suspected illicit material. This suggests Mastercard and Visa are failing to take reasonable steps, through their compliance programs with their financial partners, to prohibit their products and networks from functioning as the "financial gateway" to accessing illicit material on these sites. FinCEN is well-positioned to take steps to limit abuse on the platform under its Title 31 authority.

These actions (including evaluating whether Visa and Mastercard are in violation of the AML program requirement imposed on "Operators of a Credit Card System") to limit trafficking are consistent with the guidance in your national priority list. Members of your senior leadership team have been briefed in detail about opportunities to evaluate Visa and Mastercard's compliance with the AML program requirement, as have members of MLARS and other relevant stakeholders. Moving forward with a regulatory approach, as opposed to a Department of Justice-led Title 18 approach, awaits FinCEN's leadership and action. (AIP briefed FinCEN leadership on this issue September 20, 2021.)

a. So, Director Das, what steps will you commit FinCEN take to address this highly concerning problem with the credit card companies and others in the financial services sector doing business with these websites?

Answer: FinCEN is committed to addressing the heinous crimes of human trafficking, including sex trafficking, and cybercrime involving child sexual abuse and exploitation materials (CSAM). FinCEN included human trafficking and cybercrime in the first-ever AML/CFT national priorities issued in June 2021 (the Priorities). To provide guidance to covered institutions with respect to the Priorities, FinCEN, in conjunction with functional regulators, issued statements accompanying the Priorities advising banks and covered non-bank financial institutions they may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based BSA compliance programs and risk-based AML programs, respectively, including by assessing the potential risks associated with products and services they offer, the customers they serve, and the geographic areas in which they operate. FinCEN is working, in close consultation with the federal functional regulators, on promulgating regulations required under the AML Act to mandate that all covered financial institutions with AML/CFT Program requirements, including credit card operators, incorporate those priorities into their risk-based programs.

Credit card operators have a clear responsibility under the BSA and the regulations thereunder[1] to implement an AML program reasonably designed to prevent the operator of a credit card system from being used to facilitate money laundering. Additionally, banks that process credit card transactions have a requirement to report any suspicious

[1] *See* 31 CFR 1028.210

activity that involves or aggregates to at least $5,000 and that the bank believes is relevant to the possible violation of law or regulation, as described in FinCEN's regulations.

FinCEN has focused industry's attention on human trafficking and CSAM issues through the issuance of a supplemental advisory on Human Trafficking in October 2020,[2] and a special notice[3] issued in September 2021 that drew attention to the alarming increase in CSAM-related activity as children spent more time online during the pandemic. Furthermore, FinCEN's efforts, particularly on CSAM, have included working directly with financial services and technology firms to support the development and use of new, innovative tools and solutions for detecting related financial activity and supporting law enforcement efforts to take down the criminal networks and individual purveyors of these materials.[4]

FinCEN will continue to support law enforcement and provide guidance to financial institutions to assist them in preventing transactions in support of this illegal activity. FinCEN will also continue to foster information sharing among financial institutions consistent with Section 314(b) of the USA PATRIOT Act, which we know leads to better detecting and reporting of suspicious transactions potentially linked to this activity.

b. To follow up, what can Congress do to support these initiatives with a permanent legislative solution?

Answer: FinCEN already has authority under the BSA to address the financial aspects of crimes, including human trafficking and cybercrime, and we are not seeking any additional authority from Congress in this regard at this time.

Representative Blaine Luetkemeyer

a. Acting Director Das, in your recent rulemaking on the Corporate Transparency Act, you drastically expanded who is classified as a beneficial owner within the ownership, and control prongs of the definition.

Instead of simply requiring the reporting of anyone with a 25% equity stake in a company, FinCEN has decided to create the term "ownership interest" which includes equity interest, as well as capital or profit interest, warrants or rights, and options to acquire equity or capital. Why have you decided to drastically expand this definition beyond the statutory requirements, and beyond the Customer Due Diligence Rule?

Answer: Focusing on more than equity interests is consistent with the definition of beneficial owner set out in the Corporate Transparency Act (CTA), specifically in 31

[2] See FinCEN, "FinCEN Advisory, FIN-2020-A008," (October 15, 2020), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a008
[3] See FinCEN, "FinCEN Calls Attention to Online Child Sexual Exploitation Crimes," (September 16, 2021), https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf
[4] See Alliance for Innovative Regulation TechSprint on Financial Crime: Using Traceability in Crypto to Combat CSAM," (October 19-23, 2020), https://regulationinnovation.org/crypto-techsprint/

U.S.C 5336(a)(3)(A)(ii), which uses the term "ownership interest." In issuing the final reporting rule, FinCEN considered a wide range of comments, including those related to the definition of beneficial owner and "ownership interest" in developing its regulatory definitions of these terms.[5]

Commenters were divided on whether FinCEN should treat the term "ownership interest" as though it was synonymous with the term "equity interest" found in the 2016 Customer Due Diligence Rule (CDD Rule) and whether FinCEN should adhere to the model of the 2016 CDD Rule in developing the BOI reporting rule. In the preamble to the final BOI reporting rule, FinCEN explained in detail the reasons for its view that BOI reporting requirements under the CTA should not follow the model of the 2016 CDD Rule.

The CTA does not limit beneficial ownership interests to equity, and does not use the word "equity" with respect to ownership interests. The statute also explicitly contemplates other direct and indirect forms of ownership through additional "arrangement[s]." This broad scope reflects a complex reality in which one can own interests in entities through myriad layered instruments and circumstances as highlighted in the CTA's Sense of Congress.[6] FinCEN endeavored to reasonably interpret the statutory language in defining beneficial ownership in the final rule.

a. Do you think these additional requirements will make it harder on businesses to comply with the rule?

Answer: In its recently issued final BOI reporting rule, FinCEN took into consideration all comments, and is mindful of the CTA's directive to minimize burdens on reporting companies, while seeking to establish a highly useful database for law enforcement.

FinCEN believes that the definition of ownership interest is structured in a way that will make it relatively straightforward for the majority of small businesses with a simple ownership structure to file and update reports.

While defining "ownership interest" to mean only equity interests may make identifying beneficial owners more straightforward in some cases and probably result in fewer individuals identified, it would enable individuals to maintain ownership through other means, thereby undercutting the CTA's purpose of uncovering malign actors using entities to conceal their involvement in illicit activities and "generat[ing] a database that is highly useful to national security, intelligence, and law enforcement agencies and

[5] The CTA itself, not FinCEN, created the term "ownership interest." *See* 31 U.S.C. 5336(a)(3)(A)(ii) ("The term 'beneficial owner' means, with respect to an entity, an individual who, directly or indirectly, through a contract, arrangement, understanding, relationship or otherwise…owns or controls not less than 25 percent of the *ownership interests* of the entity…" (emphasis added)).

[6] *See* Corporate Transparency Act, Title LXIV of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283 (January 1, 2021), Section 6402(4), "[m]oney launderers and others involved in commercial activity internationally conduct transactions through corporate structures in order to evade detection, and may layer such structures, much like Russian nesting "Matryoshka" dolls, across various secretive jurisdictions. . ."

Federal functional regulators."[7]

b. Will financial institutions be forced to collect more information from prospective business owners because of this change in the rule?

Answer: FinCEN will address how requirements under the 2016 CDD Rule might change when we propose revisions to the CDD Rule consistent with CTA requirements. The CTA requires that these revisions be published no later than one year after the effective date of the reporting rule.

c. Furthermore, FinCEN has decided anyone with "substantial control" of a company includes senior officers of the company, anyone with influence direction or decision over important matters, or any other form of substantial control of the company. This definition is well beyond the CDD rule and gives FinCEN significant additional authority. Treasury already has a definition of "control" under the Defense Production Act. In my mind, any definition of "substantial control" would be much narrower. Why do you think the definition of substantial control should be significantly broader?

Answer: In developing the final BOI reporting rule, FinCEN carefully considered comments specifically on the "substantial control" definition received in response to the BOI reporting NPRM.

The preamble of the final BOI reporting rule articulates FinCEN's basis for deviating from the approach in the 2016 CDD Rule. First, FinCEN concluded that incorporating the 2016 CDD Rule's numerical limitation for identifying beneficial owners via substantial control is inconsistent with the CTA's objective of establishing a comprehensive BOI database for all beneficial owners of reporting companies. Second, with respect to the reporting of beneficial owners who may exercise substantial control over an entity, any artificial ceiling could become a means of evasion or circumvention. Requiring reporting companies to identify all individuals who exercise substantial control would—as the CTA envisions—provide law enforcement and others a much more complete picture of who makes important decisions at a reporting company.

Representative Ted Budd

1. FinCEN should promote and protect innovation in digital assets space and ensure that the United States' lead in this promising industry. Does the mere act of a software developer creating and potentially selling a convertible virtual currency (CVC) cause the developer to be a money service business (even if it does not have the power to redeem the CVC) and the application or use of the CVC was peer-to-peer and non-financial?

   Answer: FinCEN is committed to working with you and other Members of Congress to ensure that FinCEN continues to support responsible innovation while protecting the integrity of the U.S. financial system and safeguarding U.S. national security. In 2013

[7] CTA, Section 6402(8)(C).

and 2019, FinCEN issued CVC-focused guidance describing when certain entities may be subject to regulation as money service businesses (MSB). This guidance discusses the role of software developers, and the creators of convertible virtual currency and distributed applications. Whether a specific entity is considered an MSB is a matter of facts and circumstances.

Representative Lance Gooden

1. Investigators and veteran law enforcement professionals conclude that it is highly likely OnlyFans.com is facilitating sexual crimes against innocent women, children, and teens, which crimes are being accessed through U.S. financial institutions. FINCEN has direct statutory and regulatory authority over the credit card and payment networks that are providing the financial gateway for child sexual abuse material (CSAM) and sex trafficking on the OnlyFans platform.

    a. Is FINCEN concerned with the alarming rate at which child porn and sex trafficking is occurring online, and do you believe payment processors who facilitate this transaction or companies like Amazon Web Services who host illicit content are generating profit for human traffickers?

    Answer: FinCEN is committed to addressing the heinous crimes of human trafficking and cybercrime involving child sexual abuse and exploitation materials (CSAM). FinCEN included human trafficking and cybercrime in the first-ever AML/CFT national priorities issued in June 2021 (the Priorities). To provide guidance to covered institutions with respect to the Priorities, FinCEN, in conjunction with other functional regulators, issued statements accompanying the Priorities advising banks and covered non-bank financial institutions they may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based BSA compliance programs and risk-based AML programs, respectively, including by assessing the potential risks associated with products and services they offer, the customers they serve, and the geographic areas in which they operate. FinCEN is working, in close consultation with the federal functional regulators, on promulgating regulations required under the AML Act to oblige all covered financial institutions with AML/CFT Program requirements, including credit card operators, to incorporate those priorities into their risk-based programs.

    Credit card operators have a clear responsibility under the BSA[8] to implement an AML program reasonably designed to prevent the operator of a credit card system from being used to facilitate money laundering. Additionally, banks that process credit card transactions have a requirement to report any suspicious activity that involves or aggregates to at least $5,000 and that the bank believes is relevant to the possible violation of law or regulation, as described in FinCEN's regulations.

    FinCEN has focused industry's attention on human trafficking and CSAM issues through

[8] *See* 31 CFR 1028.210

the issuance of a supplemental advisory on Human Trafficking in October 2020,[9] and a special notice[10] issued in September 2021 that drew attention to the alarming increase in CSAM-related activity as children spent more time online during the pandemic. Furthermore, FinCEN's efforts, particularly on CSAM, have included working directly with financial services and technology firms to support the development and use of new, innovative tools and solutions for detecting related financial activity and supporting law enforcement efforts to take down the criminal networks and individual purveyors of these materials.[11]

FinCEN will continue to support law enforcement and provide guidance to financial institutions to assist them in preventing transactions in support of this illegal activity. FinCEN will also continue to foster information sharing among financial institutions consistent with Section 314(b) of the USA PATRIOT Act, which we know leads to better detecting and reporting of suspicious transactions potentially linked to this activity.

b. Do you have any plans to review the AML programs of Amazon Web Services which host child pornography or the payment processors like Visa and Mastercard which allow human traffickers to profit from the sexual exploitation of children?

Answer: FinCEN takes such allegations seriously and works closely with other regulators to ensure law enforcement has access to BSA reporting to pursue such crimes.

2. The Treasury Department's 2022 National Terrorist Financing Risk Assessment Report revealed terrorist groups have misused tax-exempt organizations to support their activities. This has included instances where donations to a charitable organization were intentionally routed to terrorist groups and where a charitable organization knowingly or intentionally provided logistical services, recruitment, or otherwise facilitated support to a terrorist group in a conflict zone.

Previously, I have raised concerns about foreign adversaries like China, Russia, and Iran using tax-exempt organizations to push misinformation and launder money. Additionally, there are countless examples of "non-profits" participating in illicit financial activity in the United States.

a. Do you believe that there needs to be greater scrutiny of overseas partners of US charities? How could domestic charities collaborate better with law enforcement on terror finance and related crimes?

Answer: FinCEN takes very seriously the need for financial institutions to appropriately and consistently assess the unique risks of individual customers, including tax-exempt, non-profit, and charitable organizations. To assist in that effort, FinCEN and the Federal

[9] See FinCEN, "FinCEN Advisory, FIN-2020-A008," (October 15, 2020), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a008
[10] See FinCEN, "FinCEN Calls Attention to Online Child Sexual Exploitation Crimes," (September 16, 2021), https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf
[11] See Alliance for Innovative Regulation TechSprint on Financial Crime: Using Traceability in Crypto to Combat CSAM," (October 19-23, 2020), https://regulationinnovation.org/crypto-techsprint/

Banking Agencies (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration) issued a joint statement in November 2020.[12]

That joint statement stated, "The Agencies remind banks that the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for money laundering, terrorist financing, or sanctions violations. The Agencies remind banks that charities vary in their risk profiles and should be treated according to such profiles. Banks should apply the risk-based approach and evaluate charities according to their particular characteristics to determine whether they can effectively mitigate the potential risk some charities may pose. This approach helps to minimize illicit finance risks."

The statement also goes on to provide additional guidance regarding the potential risks depending upon the nature of the charity's activities: "U.S. charities that operate and provide funds solely to domestic recipients generally present low TF risk. However, U.S. charities that operate abroad, provide funding to, or have affiliated organizations in conflict regions, can present potentially higher TF risks."

On your second question, I defer to law enforcement to address how domestic charities could better collaborate with law enforcement on terror finance and related crimes.

b. Under FinCEN's existing authority do you believe you have enough tools and resources to detect illicit financial activity in the tax-exempt sector?

Answer: FinCEN uses its existing BSA authority to work with other Treasury components, interagency partners, and other stakeholders on a range of efforts to combat illicit finance. Law enforcement agencies have access to BSA reporting for illicit finance-related investigations, including for those implicating the tax-exempt sector. FinCEN is not seeking any additional authority from Congress in this regard at this time. We continue to study the issue in the context of the review and strategy required under Section 6215 of the Anti-Money Laundering Act of 2020, which may help us identify any additional measures, tools, or resources necessary to augment our efforts in this area.

Representative Pete Sessions

1. Following up on a letter I sent you last week, I'm hopeful that FinCEN can commit to updating or providing clarity around its 2019 CVC (or convertible virtual currencies) guidance.

   Without a doubt, the world of open-source software and blockchain networks has changed mightily since FinCEN first issued this guidance. The decentralized web, also

[12] *See* FinCEN, "FinCEN and Federal Banking Agencies Clarify BSA Due Diligence Expectations for Charities and Non-Profit Customers," (November 19, 2020), https://www.fincen.gov/news/news-releases/fincen-and-federal-banking-agencies-clarify-bsa-due-diligence-expectations

known as Web 3.0, has increased by leaps and bounds, as has the number of users and use cases. Among them are file storage, digital artwork, VPN internet access, video streaming, music… the list goes on.

I'm hopeful it's clear to FinCEN that these 'peer-to-peer' applications involving non-financial goods and services do not constitute money transmission. It's time to update the guidance. We have an opportunity to promote innovation in Texas and around the country. These companies should be looking to hire programmers and engineers, not lawyers. And you can help make that happen Mr. Das.

a. Do I have a commitment from you and your staff to work with me on this?

Answer: FinCEN is committed to working with you and other Members of Congress to ensure that FinCEN continues to support responsible innovation while protecting the integrity of the U.S. financial system and safeguarding U.S. national security. FinCEN regularly monitors trends and typologies in the digital asset and technology sectors, to include developments and innovations with blockchain and distributed ledger technologies. Treasury committed to leading an illicit finance risk assessment on decentralized finance in the "Action Plan to Mitigate Illicit Finance Risks for Digital Assets," pursuant to Executive Order 14067 and issued a related Request for Comment to support this effort.