FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW THE FEDERAL GOVERNMENT WEAPONIZED THE BANK SECRECY ACT TO SPY ON AMERICANS

Interim Staff Report of the

Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives

December 6, 2024

EXECUTIVE SUMMARY

Financial data can tell a person's story, including one's "religion, ideology, opinions, and interests"[1] as well as one's "political leanings, locations, and more."[2] Because of this data's usefulness, federal law enforcement agencies increasingly coordinate with financial institutions to secure even greater access to Americans' private financial information, often without legal process, and use federal laws like the Bank Secrecy Act (BSA) to do so. This interim report continues the oversight of the Committee on the Judiciary and its Select Subcommittee on the Weaponization of the Federal Government into financial surveillance in the United States. Based on nonpublic documents, this report sheds new light on the decaying state of Americans' financial privacy and the federal government's widespread, warrantless surveillance programs.

The Committee and Select Subcommittee began this investigation into government-led financial surveillance after a whistleblower disclosed that following the events of January 6, 2021, Bank of America (BoA), voluntarily and without legal process, provided the Federal Bureau of Investigation (FBI) with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region around that time.[3] In response to these allegations and corroborating testimony from FBI officials, the Committee and Select Subcommittee requested documents from BoA and six other national financial institutions about the provision of Americans' private financial information to federal law enforcement without legal process.[4] On March 6, 2024, the Committee and Select Subcommittee released an interim report revealing that federal law enforcement had used sweeping search terms like "MAGA" and "TRUMP" to target Americans and even treated purchases of religious texts or firearms as indicators of "extremism."[5] That report detailed how federal law enforcement derisively viewed American citizens—treating Americans who expressed opposition to firearm regulations, open borders, COVID-19 lockdowns, vaccine mandates, and the "deep state" as potential domestic terrorists.[6]

Following these revelations, the Committee and Select Subcommittee requested additional documents and communications from seventeen different entities, including national banks, crowdfunding sites, money service businesses, and the U.S. Treasury Department, to further examine the federal government and financial institutions' information-sharing relationship and to determine whether the federal government was abusing its access to Americans' sensitive financial information.[7] To date, the Committee and Select Subcommittee have reviewed over 48,000 pages of documents and conducted three additional transcribed interviews.

---

[1] *California Bankers Association v. Shultz*, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting).
[2] Nicholas Anthony, *What Does Financial Privacy Mean for Liberty?*, CATO Institute (Jul. 10, 2023).
[3] Transcribed Interview of Mr. George Hill, former Supervisory Intelligence Analyst, FBI at 74-75 (Feb. 7, 2023).
[4] *See*, *e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (May 25, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Jamie Dimon, Chief Exec. Officer, JPMorgan Chase & Co. (Jun. 12, 2023).
[5] *See* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).
[6] *Id.*
[7] *See generally, e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (Apr. 24, 2024).

The information obtained during the Committee and Select Subcommittee's investigation, and detailed in this report, is concerning. Documents show that federal law enforcement increasingly works hand-in-glove with financial institutions, obtaining virtually unchecked access to private financial data and testing out new methods and new technology to continue the financial surveillance of American citizens.

- **The FBI has manipulated the Suspicious Activity Report (SAR) filing process to treat financial institutions as *de facto* arms of law enforcement, issuing "requests," without legal process, that amount to demands for information related to certain persons or activities it considers "suspicious."** [8] With narrow exception, federal law does not permit law enforcement to inquire into financial institutions' customer information without some form of legal process.[9] The FBI circumvents this process by tipping off financial institutions to "suspicious" individuals and encouraging these institutions to file a SAR—which does not require any legal process—and thereby provide federal law enforcement with access to confidential and highly sensitive information.[10] In doing so, the FBI gets around the requirements of the Bank Secrecy Act (BSA), which, per the Treasury Department, specifies that "it is . . . *a bank's responsibility*" to "file a SAR whenever *it* identifies 'a suspicious transaction relevant to a possible violation of law or regulation'"[11] While at least one financial institution requested legal process from the FBI for information it was seeking,[12] all too often the FBI appeared to receive no pushback. In sum, by providing financial institutions with lists of people that it views as generally "suspicious" on the front end, the FBI has turned this framework on its head and contravened the Fourth Amendment's requirements of particularity and probable cause.[13]

- **In the days and weeks after January 6, 2021, the FBI coordinated with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) to encourage financial institutions across the country to scour their data and file SARs on hundreds of Americans, if not more, without any clear criminal nexus.**[14] Documents reveal that at least one financial institution took the initiative and reached out to FinCEN with an idea that would "support the Bureau's efforts to address the acute threat of

[8] *See, e.g.,* Transcribed Interview of Mr. Peter Sullivan at 29 (Apr. 9, 2024) (discussing the FBI's sharing of fact-based patters with financial institutions to identify potential threats); *see also, e.g.,* Email from Peter Sullivan, FBI, to FBI employee and Bcc'd recipient [Redacted] at Santander (Jan. 15, 2021 3:25 PM) (SBNA_HJC_0001084); Email from Peter Sullivan, FBI, to FBI employee and Bcc'd recipients (Jan. 15, 2021 10:25 AM) (SCB-00002713).
[9] See, e.g., 12 U.S.C. § 3413(g).
[10] *See* Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of the Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) ("SARs contain personally identifiable information about individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation . . . .")
[11] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2, 4 (Feb. 9, 2024) (emphasis added) (citing 31 U.S.C. § 5318(g)(1)).
[12] *See, e.g.*, Email from [Redacted], Standard Chartered, to Peter Sullivan, FBI, and FBI employee (Apr. 20, 2021, 2:52 PM) (SCB-00002923).
[13] *See* U.S. CONST. amend. IV.
[14] *See* Transcribed Interview of Mr. Peter Sullivan at 31-32, 34-35 (Apr. 9, 2024).

domestic terrorism."[15] That financial institution encouraged FinCEN to use SARs as the basis for issuing Patriot Act 314(a) requests, which allows FinCEN "to canvas the nation's financial institutions for potential lead information" from "more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering."[16]

- **The government's access to Americans' private financial data is widespread and virtually unchecked.** In 2023, financial institutions filed 4.6 million SARs and 20.8 million Currency Transaction Reports (CTRs) with FinCEN, which are accessible to government officials for querying and downloading via various programs.[17] According to FinCEN, at least 25,000 authorized users across federal, state, and local government have warrantless access to these filings, known as BSA data, through the FinCEN Query program.[18] In 2023, government officials ran 3,362,735 searches of the filings in the FinCEN Query program.[19] In addition to the FinCEN Query program, approximately 27,000 federal officials have access to BSA data through the Agency Integrated Access (AIA) program that allows certain federal agencies to download the data onto their own systems.[20] In total, according to FinCEN, "472 federal, state, and local law enforcement, regulatory, and national security agencies have access to BSA reports . . . ."[21]

- **Financial institutions and FinCEN are expanding their capacity to surveil Americans through new, confidential projects and emerging technologies.** Officially, the Bank Secrecy Act Advisory Group (BSAAG) serves as an advisory body to the Treasury Department on issues related to the BSA.[22] However, in practice, documents obtained by the Committee and Select Subcommittee indicate that it is also a tool for federal law enforcement and financial institutions to monitor the private, financial data of American citizens.[23] Previously confidential BSAAG documents indicate that it is advancing plans that would require Americans to have a digital identification to access financial services, testing artificial intelligence to surveil Americans' financial activity, and working towards even closer coordination between financial institutions and federal law enforcement.

---

[15] *See* Email from [Redacted], MUFG, to FinCEN employee (Jan. 13, 2021, 6:41 PM) (MUFG-0000248-249).
[16] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN'S 314(A) FACT SHEET (Feb. 26, 2019).
[17] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).
[18] *Id.* at 3.
[19] Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 25, 2024, 5:03 PM).
[20] Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024, 2:44 PM). FinCEN "does not have an exact contemporaneous count of the number of [government] users" with AIA access. *See* Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 25, 2024, 5:03 PM).
[21] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).
[22] Bank Secrecy Act Advisory Group; Solicitation of Application for Membership, 88 Fed. Reg. 9329 (Financial Crimes Enforcement Network Feb. 13, 2023).
[23] FINANCIAL CRIMES ENFORCEMENT NETWORK, CHARTER OF THE BANK SECRECY ACT ADVISORY GROUP, https://www.fincen.gov/sites/default/files/shared/charter.pdf (last visited Oct. 10, 2024).

All Americans should be disturbed by how their financial data is collected, made accessible to, and searched by federal and state officials, including law enforcement and regulatory agencies. With the rise in e-commerce and the widespread adoption of cash alternatives like credit cards or peer-to-peer payment services, the future leaves very little financial activity beyond the purview of modern financial institutions or the government's prying eyes. This is because, as a condition of participating in the modern economy, Americans are forced to disclose details of their private lives to a financial industry that has been too eager to pass this information along to federal law enforcement.

The Committee's and Select Subcommittee's investigation makes clear that federal law enforcement has taken advantage of this dynamic by deploying financial institutions as arms of federal law enforcement, directing financial institutions to profile Americans using the typologies it distributes or urging financial institutions to identify any "suspicious activity" an individual may have engaged in.[24] As promoted by the BSAAG, this surveillance will be catalyzed by even greater government entanglement with financial institutions as they begin to integrate new technology to more effectively track their customers' financial habits. Absent renewed safeguards, the federal government and financial institutions will continue to siphon off Americans' sensitive financial data, place it into the hands of bureaucrats, and erode any remaining semblance of financial privacy in the United States.

[24] STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).

TABLE OF CONTENTS

Documents obtained by the Committee and Select Subcommittee demonstrate that federal law enforcement increasingly relies on financial institutions for highly sensitive information about Americans without legal process. Federal law enforcement has effectively deputized financial institutions to advance its investigations and to gain access to the information that financial institutions possess. As financial institutions' capacity to track and gather data on Americans continues to increase, federal law enforcement will continue to be incentivized to rely on banks for easy access to sensitive information about Americans' private lives.

A. The reporting requirements of the Bank Secrecy Act turn financial institutions into confidential informants that are required to secretly report Americans' financial activities to the federal government.

Enacted by Congress in 1970, the Bank Secrecy Act (BSA)[25] and succeeding legislation are "'the primary U.S. anti-money laundering (AML) law[s]' regulating financial institutions,"[26] and that authorize the Treasury Department to impose far-reaching reporting obligations on businesses and financial institutions.[27] The BSA is primarily enforced by the Treasury Department's Financial Crimes Enforcement Network (FinCEN).[28] According to FinCEN, its mission "is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security . . . ."[29] Consistent with that mission, the BSA is touted as the "principal U.S. law for the prevention of money laundering, terrorist financing and proliferation, and other forms of illicit financial activity."[30]

Pursuant to the BSA and other anti-money laundering laws, covered financial institutions operating in the United States—like banks—are required to file certain reports, such as Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs), with the federal government reflecting their customers' information and their financial activities.[31] A financial institution is required to file a CTR on any person who conducts a transaction over $10,000 or multiple transactions that amount to over $10,000 in a single day.[32] Likewise, the BSA "requires that a bank or other financial institution file a SAR whenever it identifies 'a suspicious transaction *relevant to a possible violation of law or regulation*.'"[33] The BSA also grants broad

[25] Pub. L. No. 91-508 (1970).
[26] JAY B. SYKES, CONG. RESEARCH SERV., R45076, TRENDS IN BANK SECRECY ACT/ANTI-MONEY LAUNDERING ENFORCEMENT (2018) (internal citation omitted).
[27] *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.
[28] FINANCIAL CRIMES ENFORCEMENT NETWORK, WHAT WE DO.
[29] FINANCIAL CRIMES ENFORCEMENT NETWORK, MISSION.
[30] Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 238 (Financial Crimes Enforcement Network Dec. 15, 2021).
[31] *See, e.g.,* 31 U.S.C. §§ 5313, 5314; *see also* Transcribed Interview of Mr. Jimmy Kirby at 46, 51 (July 18, 2024).
[32] 31 U.S.C. § 5313; 31 C.F.R. § 1010.330; *see also* FIN. CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE, https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf (last visited Sept. 26, 2024).
[33] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (emphasis added).

immunity to "[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency . . . ."[34]

The BSA's reporting requirements are also extremely broad and are not limited to potentially criminal conduct.[35] When a financial institution files a SAR, it must make sensitive information available to the Treasury Department, including "personally identifiable information about individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation."[36] These filings are ostensibly subject to "strong confidentiality protections" that purport to limit access to the highly sensitive information they contain.[37] However, despite these protections, the Treasury Department estimates that tens of thousands of government officials have warrantless access to these filings.[38]

The BSA regime creates strong incentives for financial institutions to over-file SARs about American citizens—at the cost of Americans' financial privacy. In a transcribed interview with the Committee and Select Subcommittee, FinCEN Deputy Director Jimmy Kirby explained:

> There's the mandatory requirement and then there's the ability to voluntarily file, as the statutory construct laid out by Congress really is to encourage filing. So . . . there's the ones you're required to file, but there's also very much an encouragement for people to voluntarily file beyond what they're required to file.[39]

In addition to the voluntary filing option, financial institutions have a further incentive to over-file because failing to file a SAR can result in large monetary penalties.[40] As a consequence, financial institutions often file defensively, even when there is little reason to do so.[41] This dynamic is compounded by the BSA's broad grant of immunity which protects "[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency."[42] Financial institutions are also placed under a *de facto* gag order prohibiting the revelation of "any information that would reveal that the transaction has been

---

[34] 31 U.S.C. 5318(g)(3).
[35] Transcribed Interview of Mr. Jimmy Kirby at 46 (July 18, 2024) (explaining it could involve civil law violations).
[36] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024).
[37] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024).
[38] *See* Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024, 2:44 PM).
[39] Transcribed Interview of Mr. Jimmy Kirby at 46 (July 18, 2024).
[40] *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN PENALIZES U.S. BANK OFFICIAL FOR CORPORATE ANTI-MONEY LAUNDERING FAILURES (Mar. 4, 2020) (noting that FinCEN assessed $450,000 civil penalty against U.S. Bank Official for "failure to prevent violations of the Bank Secrecy Act" and $185 million civil penalty against U.S. Bank for "willfully violating the BSA's requirements").
[41] *Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI): Hearing Before the H. Comm. on Financial Services*, 118th Cong. 4 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.).
[42] 31 U.S.C. 5318(g)(3).

reported."[43] Viewing this framework together, financial institutions frequently err on the side of over-filing.[44]

During his transcribed interview with the Committee and Select Subcommittee, Peter Sullivan, former FBI Senior Private Sector Partner for Outreach within the Strategic Partner Engagement Section, acknowledged how useful sensitive financial data can be to law enforcement.[45] He explained that "financial intelligence can illuminate a lot of deliberate information . . . it could tell the pattern of life."[46] Now, decades removed from the BSA's enactment, financial institutions are able to collect and report more granular financial data than ever, heightening privacy concerns for Americans and casting renewed doubt on the BSA's constitutionality.[47]

i. Financial institutions report millions of Americans' transactions to the federal government as part of the BSA's excessive reporting requirements.

The BSA's reporting requirements have gone far beyond providing the government with reports and records that will be "highly useful in 'criminal, tax, or regulatory investigations or proceedings.'"[48] Instead, the BSA has become a dragnet that forces financial institutions to report millions of transactions to the federal government each year for potentially "suspicious activity" without any clear nexus to unlawful behavior.[49] The staggering number of these filings demonstrate the breadth of the BSA's reporting requirements and, with it, the number of Americans' transactions that are increasingly swept up by its reach. Indeed, according to Sullivan, the reach of one single SAR can be enormous. He testified that he has seen "many SARs that have more than one individual on the SAR . . . I have seen thousands."[50]

According to FinCEN, it received over 25.4 million BSA reports from 294,000 separate financial institutions and other entities in fiscal year 2023.[51] Among those filings, FinCEN reported that it received an average of 57,000 CTRs per day.[52] Given the threshold for the reporting requirement, the volume of CTR filings should not come as a surprise. In a letter to FinCEN, the American Bankers Association (ABA) explained the absurdity of the CTR filing

---

[43] 31 U.S.C. 5318(g)(2).
[44] *See Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI): Hearing Before the H. Comm. on Financial Services*, 118th Cong. 4 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.).
[45] *See* Transcribed Interview of Mr. Peter Sullivan at 41 (Apr. 9, 2024).
[46] *Id.*
[47] *See* Norbert Michel, *Experts Agree That Financial Privacy Needs A Revamp*, FORBES (Sept. 16, 2024); *see also* Brian Knight, *Is the Bank Secrecy Act Vulnerable to Constitutional Challenge over post January 6th Data Collection?*, FINREGRAG (Feb. 26, 2024).
[48] *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Govt. of the H. Comm. on the Judiciary*, 118th Cong. 6 (2024) (testimony of Norbert Michel, Vice President and Director, CATO).
[49] *See id.* at 10.
[50] Transcribed Interview of Mr. Peter Sullivan at 100 (Apr. 9, 2024).
[51] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (June 2024) (noting that in addition to financial institutions, individuals, companies, corporations, etc. are required to report cash payments of over $10,000).
[52] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (June 2024).

threshold, stating, decades "after the inception of this threshold, $10,000 is no longer an unusually large transaction."[53] If adjusted for inflation, the $10,000 threshold—which was set more than 50 years ago—would be nearly $75,000 today.[54] The ABA observed, "CTR reports have proliferated exponentially and . . . are no longer inherently tied to combating financial crime."[55] To further illustrate, if a consumer purchased a car, furniture, jewelry, art, or made a tuition payment totaling more than $10,000, a CTR was likely filed containing the consumer's information despite there being no evidence of any suspicious activity.[56]

With respect to SAR filings, the trend is the same. FinCEN reported receiving a daily average of 12,600 SAR filings, totaling more than 4.6 million in 2023.[57] FinCEN reported "Other Suspicious Activities" as the most cited reason why a financial institution filed a SAR in 2023, making up an overwhelming portion of the annual filings—totaling 3.174 million.[58] By comparison, "money laundering" accounted for just 1.629 million reports and "terrorist financing" accounted for only 1,500 filings—the least reported reason for why a SAR was filed.[59] These data confirm that FinCEN is using the BSA and its SAR reporting requirements to collect far more than "highly useful" reports on transactions that may be related to money laundering and terrorist financing. Instead, FinCEN regularly receives information about private transactions concerning "Other Suspicious Activities" that Americans may be engaged in, completely disconnected from FinCEN's stated mission or the stated purpose of the BSA.

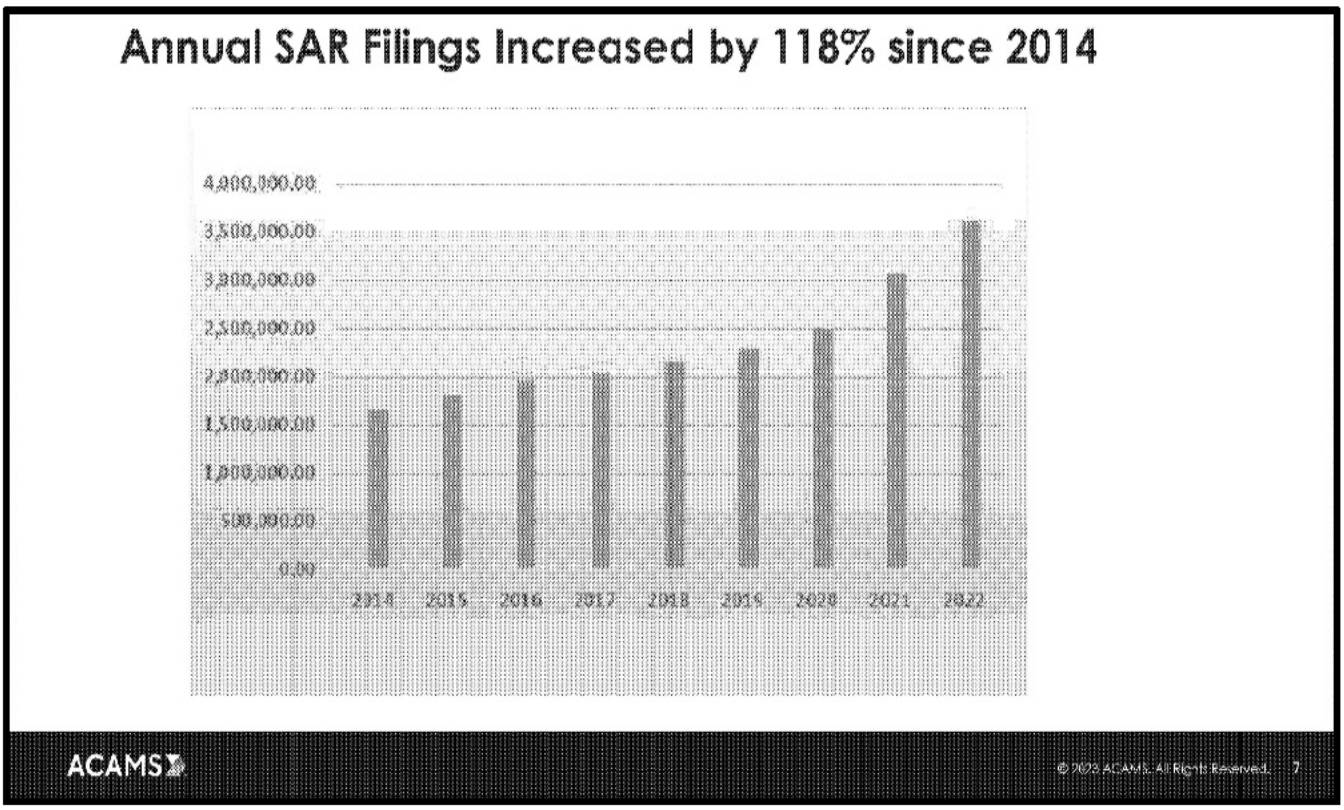
[53] American Bankers Association, *Letter to FinCEN on Information Collection Requirements relating to Currency Transaction Reports* (Apr. 5, 2024).
[54] *See* Nicholas Anthony, *How Inflation Erodes Financial Privacy*, CATO (June 10, 2022).
[55] American Bankers Association, *supra* note 53.
[56] INTERNAL REVENUE SERVICE, UNDERSTAND HOW TO REPORT LARGE CASH TRANSACTIONS (FEB. 2021).
[57] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).
[58] *Id.*
[59] *Id.*; *see also Special Report: suspicious activity reports surge; 2023 filings on pace for another record*, THOMSON REUTERS (June 9, 2023).

ACAMS slideshow on curbing Excessive SAR Filing Volumes that implicate Americans.
—Association of Certified Anti-Money Laundering Specialists

The explosion of BSA-required filings has become a topic of discussion in the industry. One of the purported leading groups in the financial crimes space is the Association of Certified Anti-Money Laundering Specialists (ACAMS), which describes itself as "the largest international membership organization for Anti-Financial Crime professionals"[60] and provides "the global gold standard in AML [Anti-Money Laundering] certifications."[61] A slideshow obtained by the Committee and Select Subcommittee shows that even ACAMS believes that SAR over-filing is a problem.[62] According to these documents, on May 9, 2023, ACAMS hosted a panel titled, "SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes."[63] In the description of the panel, "[l]ed by seasoned compliance veterans," ACAMS observed: "To paraphrase a saying about the weather, everybody complains about high SAR volumes, but nobody does anything about it," and explained that the panel's discussion would focus on "the current climate of escalating SAR filing volumes."[64] One slide from the presentation showed a 118-percent surge in SAR filings over the last decade.[65]

---

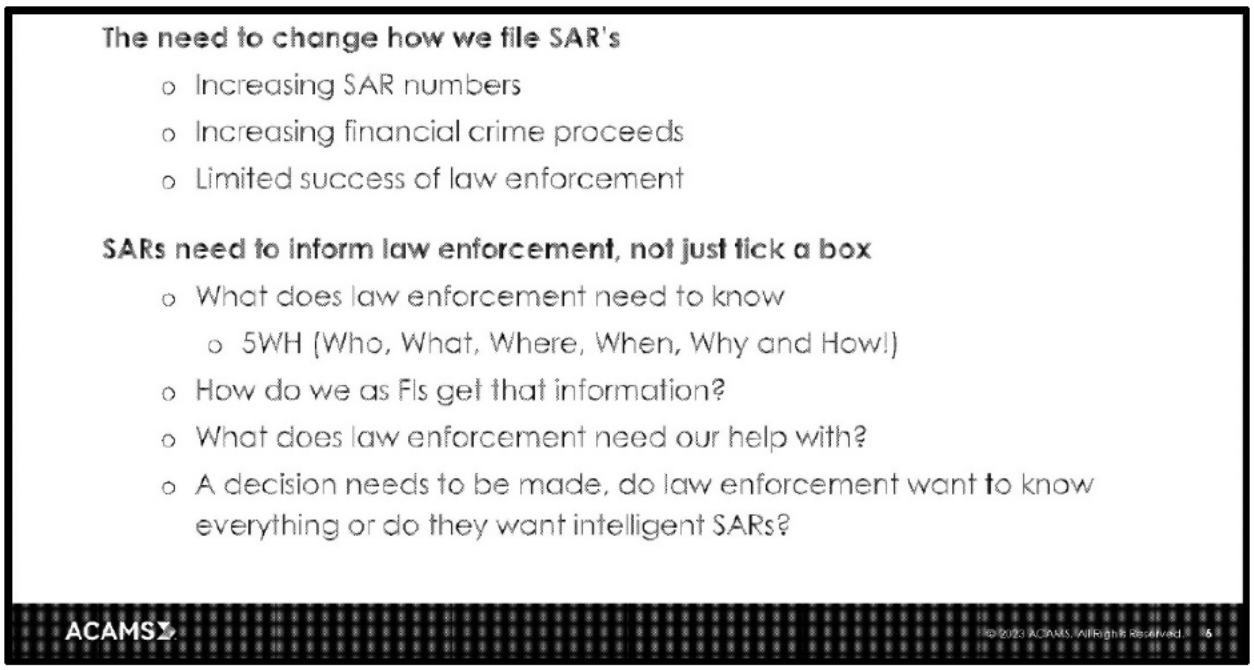
[60] ACAMS, *About Us*, https://www.acams.org/en/about#about-us-c4ffaef2 (last visited Sept. 27, 2024).
[61] ACAMS, https://www.acams.org/en (last visited Sept. 27, 2024).
[62] *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002809).
[63] Wintrust Financial Corp., Truist Financial Corp., HSBC, NICE Actimize, *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS (May 9, 2023) (118HJC_00005985).
[64] Wintrust Financial Corp., Truist Financial Corp., HSBC, NICE Actimize, *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS (May 9, 2023) (118HJC_00005985).
[65] *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002806).



SAR Filings increased by 118% from 2014 to 2022.
—Association of Certified Anti-Money Laundering Specialists

Another slide from the panel's discussion on "curb[ing] excessive filing volumes" touched on "the need to change" the BSA regime.[66] According to ACAMS, SAR numbers are increasing, despite law enforcement having "[l]imited success" in using SARs as part of their criminal investigations.[67] The ACAMS slide aptly described the over-filing problem, by inquiring "do[es] law enforcement want to know everything or do they want intelligent SARs?"[68] Under the current BSA regime, law enforcement appears to want to know everything. As this report details, financial institutions are filing millions of SARs on Americans' transactions in the hopes that it will appease law enforcement's appetite to "know everything."

[66] *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).
[67] *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).
[68] *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).



"Do[es] law enforcement want to know everything or do they want intelligent SARs?"
—Association of Certified Anti-Money Laundering Specialists

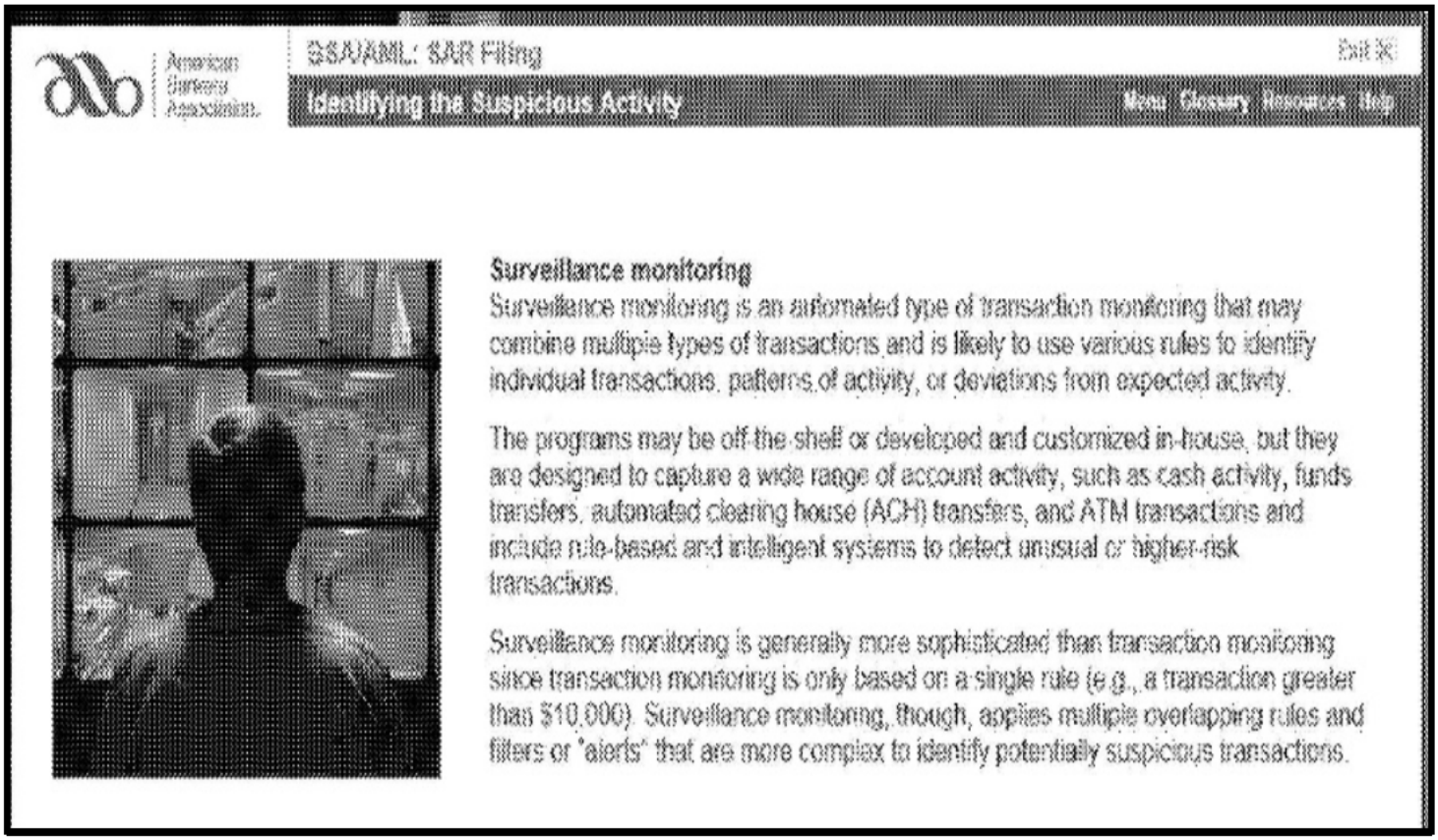
ii. In order to effectuate the BSA's requirements, financial institutions must engage in mass surveillance of Americans' private transactions.

To comply with the BSA and related requirements, banks must establish a "BSA/AML [Anti-Money Laundering] compliance program" that includes "proper monitoring and reporting processes" to "identify unusual activity" and monitor "suspicious activity."[69] These "[m]onitoring systems typically include . . . transaction-based (manual) systems, surveillance (automated) systems, or any combination of these."[70] With so much data collected by financial institutions, this monitoring is becoming increasingly widespread.

In a July 2022 presentation about these compliance programs, the ABA explained how financial institutions "identify[] the suspicious activity" using a technique called "surveillance monitoring."[71] To reinforce the point, a picture on the slide showed a figure monitoring several one-way video feeds for "suspicious" activities.[72] The slide explained that "surveillance monitoring" programs "are designed to capture a wide range of account activity, such as cash activity, fund transfers, automated clearing house (ACH) transfers, and ATM transactions and include rule-based and intelligent systems to detect unusual or higher-risk transactions."[73] With the assistance of technology, the slide noted, these systems are becoming increasingly

[69] FED. FIN. INST. EXAMINATION COUNCIL, ASSESSING COMPLIANCE WITH BSA REGULATORY REQUIREMENTS, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04 (last visited Oct. 1, 2024).
[70] *Id.*
[71] *BSA/AML: SAR Filing*, American Bankers Association (July 2022) (SBNA_HJC_0000727).
[72] *Id.*
[73] *Id.*

intelligent.[74] One report on BSA/AML compliance also noted that while "regulators do not require the use of any particular technology or system, they encourage (and expect) use of innovative technology to increase the efficacy of BSA/AML programs."[75]



"Surveillance monitoring is an automated type of transaction monitoring . . . to identify individual transactions [and] patterns of activity. . . ."
—American Bankers Association Slideshow

Americans should be rightly skeptical of a federal regime like the BSA that requires unaccountable financial institutions, on behalf of federal law enforcement, to build out a surreptitious and highly sophisticated surveillance system for monitoring and secretly flagging Americans' transactions as "suspicious" or "unusual." As the former Director of the Office of Stakeholder Integration and Engagement in the Strategic Operations Division at FinCEN explained, a bank's surveillance system is "[l]egal and required" under federal law.[76] He testified:

> Q. . . . And [are there] investigators in, particularly the banks that are large enough to have multiple employees and entire

[74] *Id.*
[75] *BSA/AML and International Trade Enforcement And Compliance Annual Update*, Gibson Dunn 97 (Feb. 7, 2024).
[76] Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 54 (May 14, 2024).

compliance units, whose job it is to search and monitor their customers' financial records for suspicious activity that must be reported?

A. Yes.

Q. And based on your experience both at a financial institution and at FinCEN, that type of monitoring by a bank, by a financial institution of its own customers' data, that's entirely legal, correct?

A. Legal and required.

Q. Legal and required?

A. Yeah.

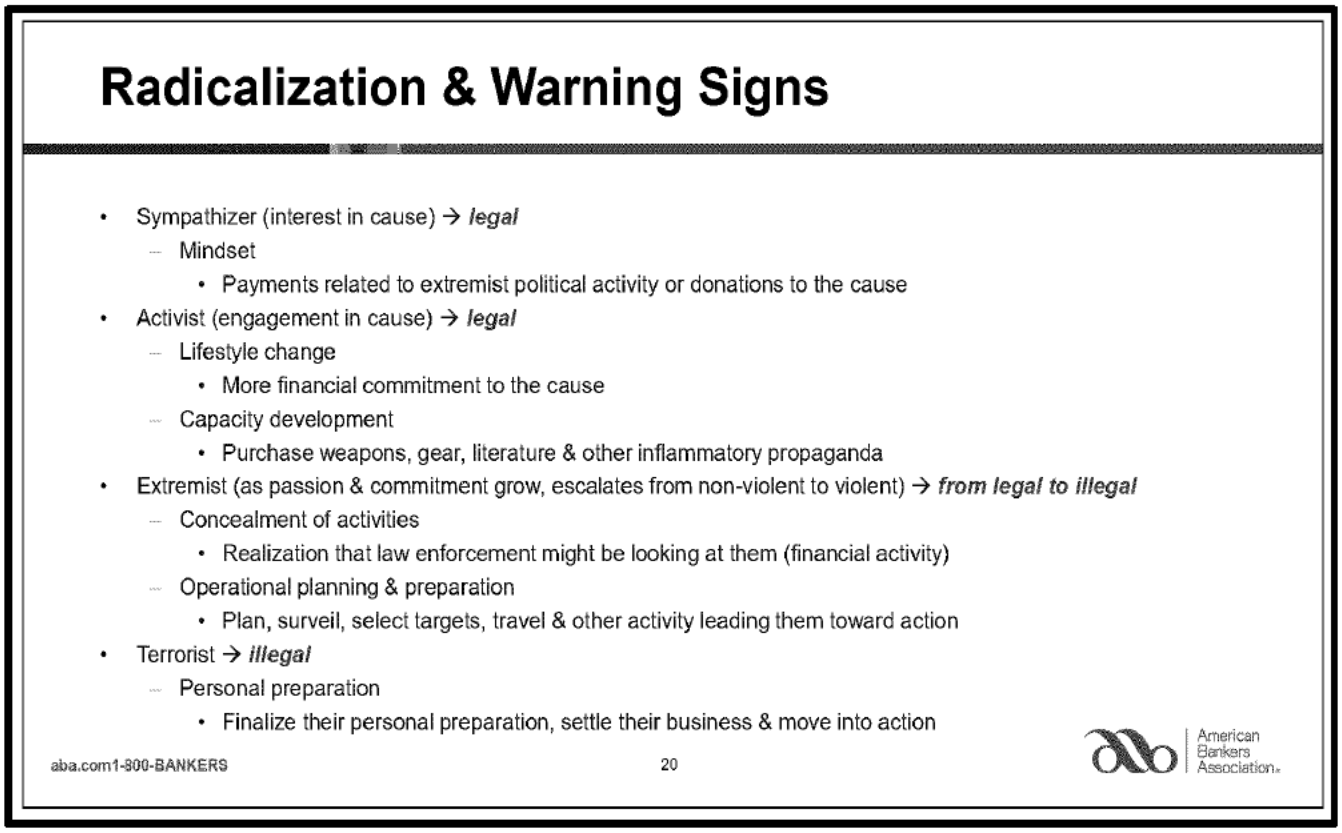
Q. No subpoenas required, no—no warrant is required?

A. Correct.[77]

The mass monitoring by financial institutions opens the door for federal law enforcement to spy on Americans' constitutionally protected activity. For example, on September 28, 2022, Peter Sullivan and a representative from Wells Fargo presented at an ABA webinar, titled "Domestic Terrorism: A Threat to the Financial System."[78] Their presentation included a slide titled "Radicalization & Warning Signs."[79] The slide illustrated how banks should review a customer's transactions, explaining the transition from a "sympathizer" of a cause (which the ABA concedes is legal), to an "activist" (which is also labeled as legal), to an "extremist" (which begins the shift from "legal to illegal"), and, ultimately, to engaging in illegal "terrorist" activities.[80] While the presentation included a disclaimer that "[b]anks don't want to interfere with customers' First Amendment rights,"[81] by highlighting transactions related to First and Second Amendment activity as an early sign of radicalization, the slide seemed to encourage financial institutions to begin tracking Americans' transactions even when they are engaged in constitutionally-protected activity. For example, the "warning signs" that the ABA suggests banks should look for include customers making "payments related to extremist political activity or donations to the cause," "more financial commitment to the cause," and the "purchase [of] weapons, gear, literature & other inflammatory propaganda," which the ABA concedes are all

[77] *Id.*
[78] Domestic Terrorism: A Threat to the Financial System, American Bankers Association (Sept. 28, 2022) (HJC118_00000502-503).
[79] *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).
[80] *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).
[81] *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000522).

"legal" activities.[82] In effect, the ABA appears to be indicating that tracking Americans' political donations, the literature they purchase, and the firearms they buy, are all a necessary prerequisite to identifying potential extremist or illegal activity.



ABA slide illustrating when financial institutions should begin tracking customers' transactions, including when engaged in "legal" activity.
—American Bankers Association Slideshow

In effect, the BSA requires financial institutions to engage in mass surveillance of Americans' transactions and report en masse their personal information and financial activities to the federal government. Once filed, federal officials, through multiple programs, have warrantless access to search through the SARs and CTRs filed on Americans.

B. The BSA and Treasury Department programs provide law enforcement officials with broad, warrantless access to Americans' financial data.

The Treasury Department claims that access to confidential BSA documents is limited in part because SARs "contain personally identifiable information, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation."[83]

[82] *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).
[83] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 1 (July 31, 2024).

Therefore, BSA "documents or the information therein should not be disclosed to, accessed by, or disseminated to unauthorized individuals in any fashion."[84] However, despite these sensitivities, tens of thousands of government personnel have widespread and warrantless access to BSA data, like SARs and CTRs, through FinCEN programs, and, in some circumstances, programs that leave FinCEN and Congress in the dark about how BSA data is used once it is accessed.

i. Thousands of law enforcement officials have warrantless access to Americans' financial information through a vast and searchable system.

A Treasury Department program known as the FinCEN Query system grants thousands of federal, state, and local law enforcement officials the ability to "easily and quickly access, query, and analyze" BSA data through a Memorandum of Understanding (MOU) with each entity.[85] FinCEN also provides access to this program, through MOUs, to employees from intelligence agencies and other external financial regulatory agencies "to conduct official agency business."[86] According to the Office of Inspector General (OIG) of the Treasury Department, FinCEN has "475 MOUs with external LE [law enforcement], intelligence, and regulatory agencies."[87] Once a "partner agenc[y]" reaches an MOU agreement with FinCEN it "identif[ies] employees for access to the system" and, once identified, the agency provides those users with a "unique login" to access the FinCEN Query system and begin running searches.[88] Users can search "first and last names or parts of addresses," as well as other "keywords" and "search terms" to "scan across all text fields."[89] Searches conducted in the FinCEN Query system are logged by FinCEN in an audit log.[90]

During his transcribed interview, FinCEN Deputy Director Kirby described how the query system works. Using his name as an example, Kirby testified that a search for "Jimmy Kirby" would reveal any "SARs that have been filed on [Jimmy Kirby] . . . to the extent a bank has filed currency transaction reports or a non-bank has filed a Form 8300 on [Jimmy Kirby], you would see those" and "any of the other BSA forms that involve [Jimmy Kirby], you would be able to see those," it would be the "universe of . . . what has been filed on [Jimmy Kirby]."[91] Indeed, because these reporting "obligations apply to U.S. financial institutions," Kirby explained, it is safe to assume that a "substantial portion," if not the "majority of the filings," involve "U.S. persons."[92] Thousands of law enforcement personnel can generally conduct these searches on the FinCEN Query system without ever needing a warrant or any legal process.[93]

---

[84] *Id.*
[85] *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, FACT SHEET FINCEN QUERY; *see also* Transcribed Interview of Mr. Jimmy Kirby at 72, 73-74 (July 18, 2024); FINANCIAL CRIMES ENFORCEMENT NETWORK, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).
[86] U.S. DEP'T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN'S MANAGEMENT OF BSA DATA – USER ACCESS REPORT 4 (Aug. 1, 2024).
[87] U.S. DEP'T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN'S MANAGEMENT OF BSA DATA - SUPPRESSION REPORT 4 (Aug. 31, 2023).
[88] Transcribed Interview of Mr. Jimmy Kirby at 73 (July 18, 2024).
[89] FINANCIAL CRIMES ENFORCEMENT NETWORK, FACT SHEET FINCEN QUERY.
[90] Transcribed Interview of Mr. Jimmy Kirby at 73 (July 18, 2024).
[91] *Id.* at 74-75.
[92] *Id.* at 78.
[93] *Id.* at 72, 74-76.

FinCEN informed the Committee and Select Subcommittee that, in 2023, there were 14,415 registered and authorized users with access to the FinCEN Query system.[94] That year, users conducted 3,362,735 million searches of the database without a warrant or legal process, amounting to an average of 9,212 searches per day.[95]

However, the FinCEN Query system, including its searches and authorized users, do not reflect a complete picture of government officials' access to, or their searches, of Americans' financial data. In fact, according to FinCEN, "FinCEN Query users represent only a fraction of users who access" BSA data.[96] In other words, the number of government searches that FinCEN reported of its BSA data, and the number of government officials with access to the BSA data, is likely much higher. Another FinCEN program, called Agency Integrated Access, provides an additional avenue for federal officials to transfer, access, and use BSA data with little to no oversight from FinCEN.

ii. FinCEN provides federal law enforcement agencies the ability to copy and transfer entire BSA data sets from FinCEN, onto their own systems, and access it without a warrant.

FinCEN's Agency Integrated Access (AIA) program provides approved federal agencies the "ability to ingest the BSA data that is filed with FinCEN" if the agency has an MOU in place with FinCEN.[97] The Treasury OIG describes AIA as the "transfer of entire copy sets of FinCEN BSA data to an external agency" by "downloading an encrypted file daily from [the] FinCEN Portal . . . ."[98] From then on, FinCEN Deputy Director Kirby explained, "those agencies control the access to that data on their systems."[99] Once a partnered agency imports the BSA data onto their system, FinCEN does not maintain "visibility" into how the agency uses the data.[100]

FinCEN informed the Committee and Select Subcommittee that "because the agencies manage [their AIA] user accounts, FinCEN does not have an exact contemporaneous count of the number of [government] users" with AIA access.[101] However, as of September 2023, FinCEN reported "approximately 27,000 authorized agency users who had access to BSA data through AIA agencies," comprising nine federal law enforcement and national security agencies, including the FBI, Internal Revenue Service (IRS), National Security Agency (NSA), United States Secret Service (USSS), Immigration and Customs Enforcement (ICE), Organized Crime and Drug Enforcement Task Forces (OCDETF), National Counterterrorism Center (NCTC), and

[94] Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 8, 2024 10:48 AM).
[95] *Id.*
[96] U.S. DEP'T OF TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2022.
[97] Transcribed Interview of Mr. Jimmy Kirby at 72, 81 (July 18, 2024).
[98] U.S. DEP'T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN'S MANAGEMENT OF BSA DATA - SUPPRESSION REPORT 1, 5 (Aug. 31, 2023).
[99] Transcribed Interview of Mr. Jimmy Kirby at 72 (July 18, 2024).
[100] *Id.* at 72, 81.
[101] Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024 2:44 PM).

one other agency whose involvement is classified.[102] With this access, these federal agencies download the "same BSA filings" onto their own systems instead of using the auditable FinCEN Query system.[103]

The very existence of the AIA program—which allows certain federal agencies to download the same data already made available through FinCEN Query—suggests that its purpose is to provide federal agencies with the ability to access and use BSA data outside the scope of the FinCEN Query system. Given that AIA access does not provide FinCEN with the "same degree of visibility" as FinCEN Query and grants the receiving agency "control [of] the access to that data," federal law enforcement appears to operate in a regulatory blind spot in its use of Americans' financial data and in an environment ripe for federal surveillance.[104]

iii. In addition to law enforcement's access to Americans' financial information, some financial institutions use third-party contractors to monitor and report on their customers' confidential transactions.

According to documents obtained by the Committee and Select Subcommittee, some financial institutions also appear to be sharing confidential BSA data with "third party vendors."[105] On February 5, 2024, the Bank Secrecy Act Advisory Group (BSAAG) shared a draft white paper with its members that "addresse[d] unique issues that arise with BSA data and third-party relationships" and "to communicate . . . clear, consistent, cross-industry guidance/practices for information security and confidentiality when sharing BSA data with third parties."[106] This white paper illustrates the concerning practice of third-party vendors with access to confidential BSA data and that are responsible for "monitoring" Americans' banking activity.

The white paper discussed "Third Party BSA Data Sharing," a practice in which financial institutions contract with vendors that offer "Financial Crimes Management" solutions, such as "transaction monitoring, customer due diligence, and other features . . . ."[107] It explained how financial institutions may use these vendors "to augment their BSA staffing" and to "assign[] tasks in the review of transaction monitoring alerts, unusual activity investigation, or even [the] SAR preparation process" despite the fact that regulators "have not addressed the question of whether information subject to SAR confidentiality rules may be shared with business relationship partners . . . ."[108] Still, financial institutions appear to be contracting with vendors

[102] Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024 2:44 PM); Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 10, 2024 11:10 AM); Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 29, 2024 10:47 AM).
[103] Transcribed Interview of Mr. Jimmy Kirby at 72, 80 (July 18, 2024).
[104] *Id.* at 72, 81-82.
[105] Email from BSAAG to BSAAG and personnel at MUFG and Golden 1 (Feb. 5, 2024, 8:42 AM) (SCHWAB_HJC_00002945).
[106] Email from BSAAG to BSAAG and personnel at MUFG and Golden 1 (Feb. 5, 2024, 8:42 AM) (SCHWAB_HJC_00002945).
[107] *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947).
[108] *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947-2948, 2952).

that offer "solutions in which BSA data, including Suspicious Activity Report (SAR) data, is stored on the business relationship partner's platform."[109] However, these practices may be violating the BSA.

As the white paper acknowledged, "Federal Functional Regulators (FFRs) and FinCEN have not issued comprehensive rules or guidance relating to sharing BSA data with third parties" and that "it is not entirely clear to what extent [a financial institution] may use [a third party's] contract resources to perform these functions consistent with SAR confidentiality rules and guidance."[110] The white paper observed the tension between keeping BSA data confidential and sharing the same information with third-party contractors:

> The sharing of BSA data with third parties carries elevated risks, beyond data privacy and security risks related to all third-party relationships. Most BSA data, by definition, is highly confidential and sensitive . . . An FI subject to BSA regulation can run afoul of the law and prudent practice by over delegating BSA-related functions to a business-relationship partner or agent without sufficient supervision, training, and oversight.[111]

Despite the legal uncertainty, security risks, and privacy concerns that sharing BSA data with third-party vendors presents for Americans' private financial data, financial institutions appear to continue doing so with the tacit approval of the federal government.

iv. FinCEN appeared to have provided an individual with unauthorized access to a financial information-sharing system.

Section 314(b) of the USA Patriot Act "permits financial institutions, upon providing notice to the United States Department of Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity."[112] As of 2020, the 314(b) program included over 7,000 financial institutions.[113] In 2020, 17,384 SAR narratives, which consist of a summary of the suspicious activity, referenced use of the 314(b) program, indicating that financial institutions actively collaborated to share information concerning potentially suspicious activity.[114] The 314(b)

---

[109] *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947).
[110] *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002950-2952).
[111] *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002959).
[112] U.S. DEP'T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, SECTION 314(B).
[113] U.S. DEP'T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, INFORMATION SHARING INSIGHTS: 314(B) PARTICIPATION AND REPORTING.
[114] U.S. DEP'T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, INFORMATION SHARING INSIGHTS: 314(B) PARTICIPATION AND REPORTING; *see also* FIN. CRIMES ENFORCEMENT NETWORK, GUIDANCE ON PREPARING A COMPLETE & SUFFICIENT SUSPICIOUS ACTIVITY REPORT NARRATIVE (explaining SAR narratives).

program requires participating financial institutions to "protect the security and confidentiality of all information . . . and only use such information for the purposes laid out" in the statute.[115]

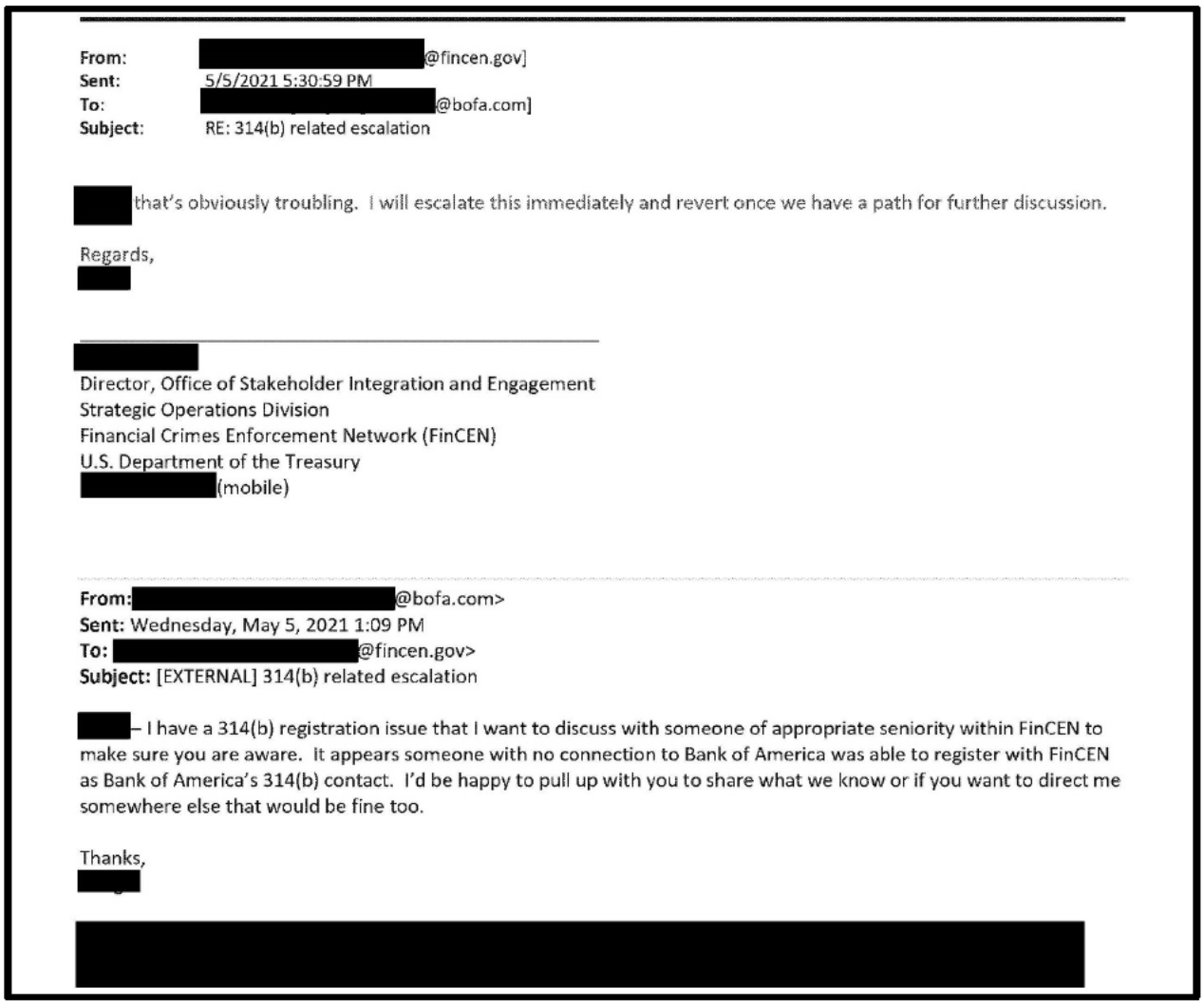
According to nonpublic documents, it appears that in at least one instance, an individual with "no connection" to a financial institution was mistakenly able to register with FinCEN as the bank's program representative and received access to the sensitive data of customers' and their transactions in this program.[116] On May 5, 2021, a BoA employee emailed the former Director of the Office of Stakeholder Integration and Engagement at FinCEN explaining that there was "a 314(b) registration issue" involving BoA.[117] He wrote:

> I have a 314(b) registration issue that I want to discuss with someone of appropriate seniority within FinCEN to make sure you are aware. It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America's 314(b) contact. I'd be happy to pull up with you to share what we know or if you want to direct me somewhere else that would be fine too.[118]

The fact that an unauthorized representative appeared to have gained access to FinCEN's 314(b) program raises the question of whether FinCEN is adequately protecting the sensitive financial data under its control and properly screening and vetting all individuals with access to this information. After BoA flagged the issue, the FinCEN employee agreed that the unauthorized access was "troubling" and would "escalate this immediately."[119]

---

[115] U.S. DEP'T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, SECTION 314(B) FACT SHEET (Dec. 2020) (citing 31 CFR 1010.540(b)(4)(i)-(ii)).
[116] Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).
[117] Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).
[118] Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).
[119] Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to personnel at Bank of America (May 5, 2021, 5:30 PM) (424HJUD00006301).



From: [redacted]@fincen.gov]
Sent: 5/5/2021 5:30:59 PM
To: [redacted]@bofa.com]
Subject: RE: 314(b) related escalation

[redacted] that's obviously troubling. I will escalate this immediately and revert once we have a path for further discussion.

Regards,
[redacted]

[redacted]
Director, Office of Stakeholder Integration and Engagement
Strategic Operations Division
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury
[redacted](mobile)

From: [redacted]@bofa.com>
Sent: Wednesday, May 5, 2021 1:09 PM
To: [redacted]@fincen.gov>
Subject: [EXTERNAL] 314(b) related escalation

[redacted]– I have a 314(b) registration issue that I want to discuss with someone of appropriate seniority within FinCEN to make sure you are aware. It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America's 314(b) contact. I'd be happy to pull up with you to share what we know or if you want to direct me somewhere else that would be fine too.

Thanks,
[redacted]

[redacted]

"It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America's 314(b) contact."
—May 5, 2021, email from Bank of America personnel to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN

Given the amount of information that can be gleaned by viewing financial data, a bad actor who gains access to the 314(b) program could use it to view, target, or disclose Americans' sensitive information. It is concerning to learn that FinCEN could mistakenly register someone with no affiliation to the bank as their representative for the 314(b) program and seemingly gain unauthorized access to the data.

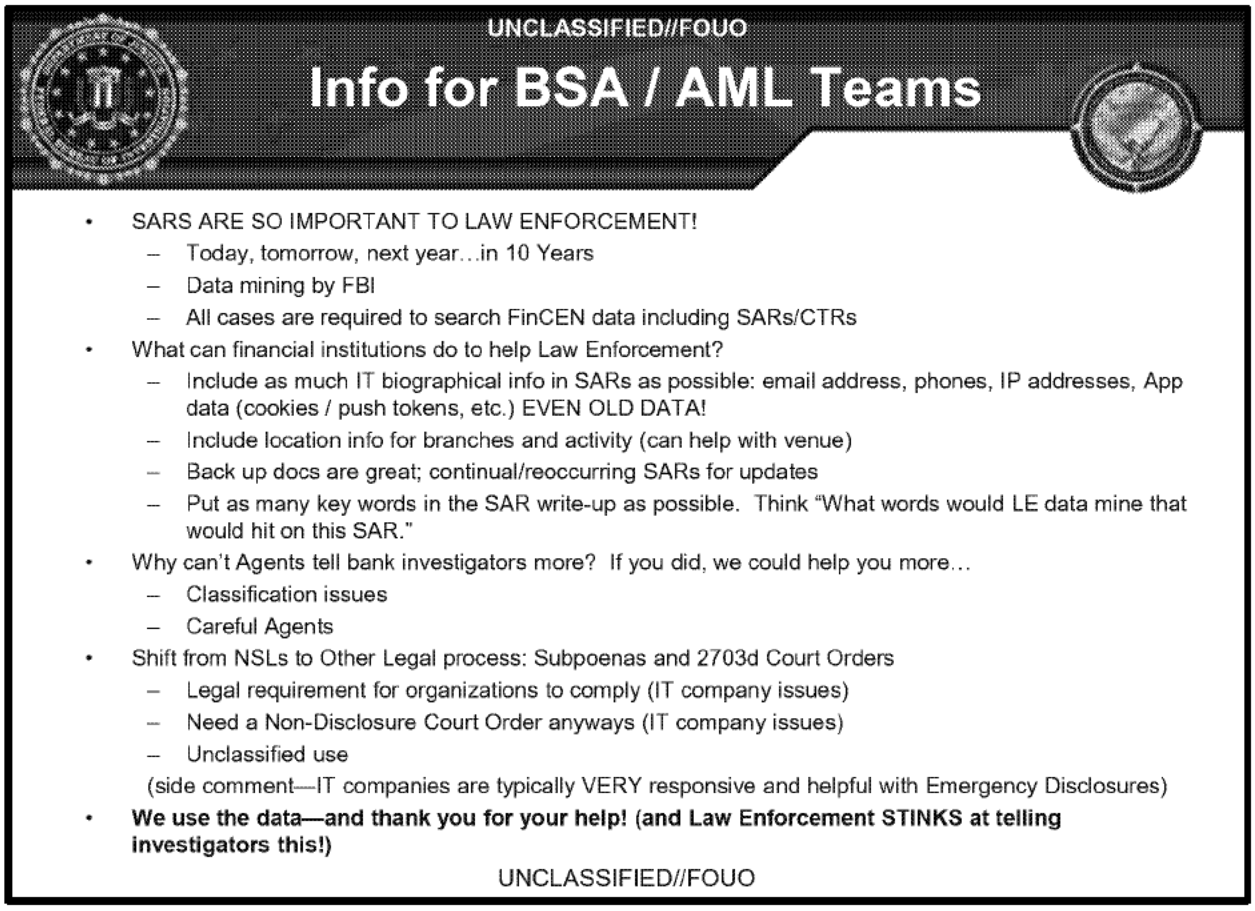
* * *

The threat of potential financial surveillance is expanding. Financial institutions are filing an ever-increasing number of confidential BSA reports like SARs and CTRs on Americans and, at the same time, the federal government is providing tens of thousands of federal, state, and local officials with warrantless access to this information and using it in undisclosed ways. As a

consequence, more people than ever before have access to Americans' sensitive financial information.

FEDERAL LAW ENFORCEMENT AND ITS PARTNERS ABUSE THE BSA'S INFORMATION-SHARING REGIME

The FBI treats the SARs filed by financial institutions as a valuable resource. The FBI has told at least one financial institution that it "data min[es]" SARs as part of its investigations and that "all cases are required to search FinCEN data including SARs/CTRs."[120] The FBI even asked financial institutions to include "as much . . . biographical info in SARs as possible: email address, phones, IP addresses, App data (cookies / push tokens, etc.) EVEN OLD DATA!"[121] It also directed financial institutions to "[p]ut as many key words in the SAR write-up as possible."[122]



UNCLASSIFIED//FOUO

Info for BSA / AML Teams

- SARS ARE SO IMPORTANT TO LAW ENFORCEMENT!
  - Today, tomorrow, next year…in 10 Years
  - Data mining by FBI
  - All cases are required to search FinCEN data including SARs/CTRs
- What can financial institutions do to help Law Enforcement?
  - Include as much IT biographical info in SARs as possible: email address, phones, IP addresses, App data (cookies / push tokens, etc.) EVEN OLD DATA!
  - Include location info for branches and activity (can help with venue)
  - Back up docs are great; continual/reoccurring SARs for updates
  - Put as many key words in the SAR write-up as possible. Think "What words would LE data mine that would hit on this SAR."
- Why can't Agents tell bank investigators more? If you did, we could help you more…
  - Classification issues
  - Careful Agents
- Shift from NSLs to Other Legal process: Subpoenas and 2703d Court Orders
  - Legal requirement for organizations to comply (IT company issues)
  - Need a Non-Disclosure Court Order anyways (IT company issues)
  - Unclassified use

  (side comment—IT companies are typically VERY responsive and helpful with Emergency Disclosures)
- **We use the data—and thank you for your help! (and Law Enforcement STINKS at telling investigators this!)**

UNCLASSIFIED//FOUO

"What words would [Law Enforcement] data mine that would hit on this SAR."
—FBI Charlotte Division Joint Terrorism Task Force Slideshow

[120] *International Terrorism*, FBI Charlotte Division Joint Terrorism Task Force (424HJUD00004507).
[121] *Id.* (emphasis in original).
[122] *Id.*

In his transcribed interview with the Committee and Select Subcommittee, the former Director of the Office of Stakeholder Integration and Engagement at FinCEN acknowledged that the SAR process sweeps in much more information than just suspicious activity.[123] He testified:

> So, again, it's instead of looking for that needle in a haystack in millions of transactions, it's let's take a narrow subset that fits certain characteristics and look at those to evaluate whether they are suspicious. . . . Are we going to be overly inclusive in looking at things that we decide are not suspicious? Absolutely. But it makes it manageable.[124]

The issue with FinCEN's "overly inclusive" approach, however, is that it subjects innocent Americans and their highly sensitive information to potential FBI scrutiny or other law enforcement investigations. The customer's information is never deleted and the customer never learns whether a financial institution has filed a SAR on them.[125]

A. Federal law enforcement has broad discretion in what it considers "suspicious" financial activity and urges financial institutions to review their customers' transactions and file reports on the activity they consider "suspicious."

In 2021, Congress codified a new program called the FinCEN Exchange "to facilitate the sharing of information between law enforcement, FinCEN, and financial institutions" to include the sharing of "typologies," "trends," and other information that financial institutions "could consider incorporating into their existing AML/CFT [Anti-Money Laundering / Countering the Financing of Terrorism] programs" in order to "identify indicia of suspicious activity."[126] FinCEN Deputy Director Kirby described the FinCEN Exchange as "probably our premier public-private partnership, and it's a way for the private sector and different parts of government to come together and share information on priority topics."[127]

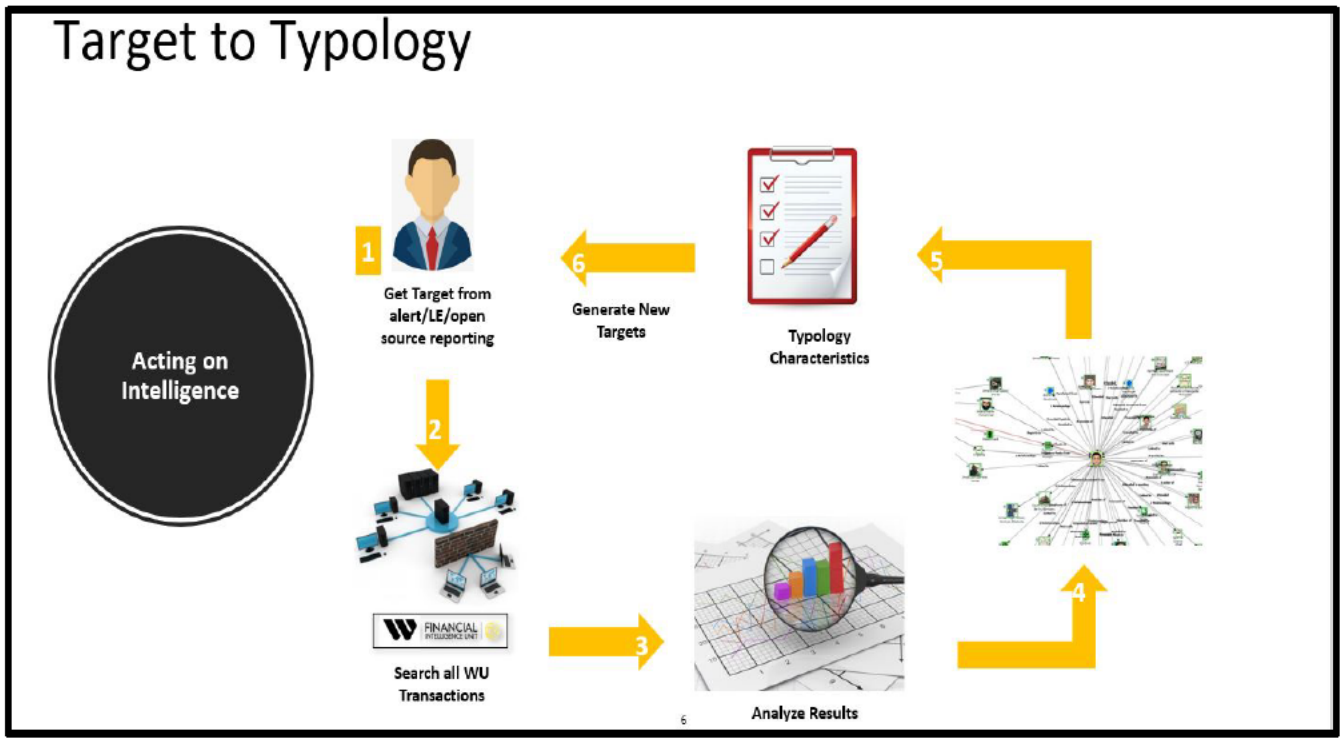
Financial institutions review the typologies, trends, and other criteria provided to them through the FinCEN Exchange and subsequently review their own customers' transactions to determine if there is reportable suspicious activity.[128] This exchange of information creates a feedback loop between the government and financial institutions that, when used appropriately, may help the government and financial institutions detect and deter fentanyl distribution, human trafficking, or terrorist financing.[129] However, as Peter Sullivan, the former FBI Senior Private

---

[123] Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 141 (May 14, 2024).
[124] *Id.*
[125] *See* Transcribed Interview of Mr. Jimmy Kirby at 78 (July 18, 2024); *see also* 31 U.S.C. 5318(g)(2) (prohibiting notification that a transaction has been reported).
[126] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3-4 (Feb. 9, 2024).
[127] Transcribed Interview of Mr. Jimmy Kirby at 15-16 (July 18, 2024).
[128] *See* Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (quoting 31 U.S.C. § 5318(g)(1)).
[129] *See* Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2-3 (Feb. 9, 2024); *see also, e.g.,* Transcribed Interview of Mr. Jimmy Kirby at 16 (July 18, 2024).

Sector Partner for Outreach within the Strategic Partner Engagement Section noted during his transcribed interview, the FBI is not limited in the kind of transactions it can suggest to financial institutions as potentially suspicious. He testified:

> Q. Are there limits in terms of the kind of transactions that you can express an interest as being possibly suspicious?
>
> A. From my law enforcement standpoint, there [are] various things that we can discuss and brainstorm. So, in that sense, you know, it varies. It's a pretty wide scope.[130]



Slide detailing the feedback loop between the government and financial institutions. —March 2024 presentation from Western Union Financial Intelligence Unit.[131]

While "it is ultimately a bank's responsibility to determine when—consistent with the BSA and its implementing regulations—a bank must file a SAR,"[132] when federal law enforcement and Treasury Department regulators share information with banks for them to "consider incorporating into their existing AML/CFT programs,"[133] financial institutions have a massive incentive to act on the intelligence they receive from government officials and

[130] Transcribed Interview of Mr. Peter Sullivan at 139 (Apr. 9, 2024).
[131] Western Union, Using Strategic Intelligence to Combat Financial Crime at 6 (2023) (PowerPoint presentation) (WesternUnion-0004941.PPTX).
[132] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 4 (Feb. 9, 2024) (emphasis added).
[133] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3 (Feb. 9, 2024) (emphasis added).

regulators. If the banks fail to file SARs that they should have, or otherwise fail to comply with the BSA by maintaining effective AML programs, they could incur civil penalties that could total hundreds of millions of dollars.[134] This is the incentive framework in which financial institutions are forced to operate.

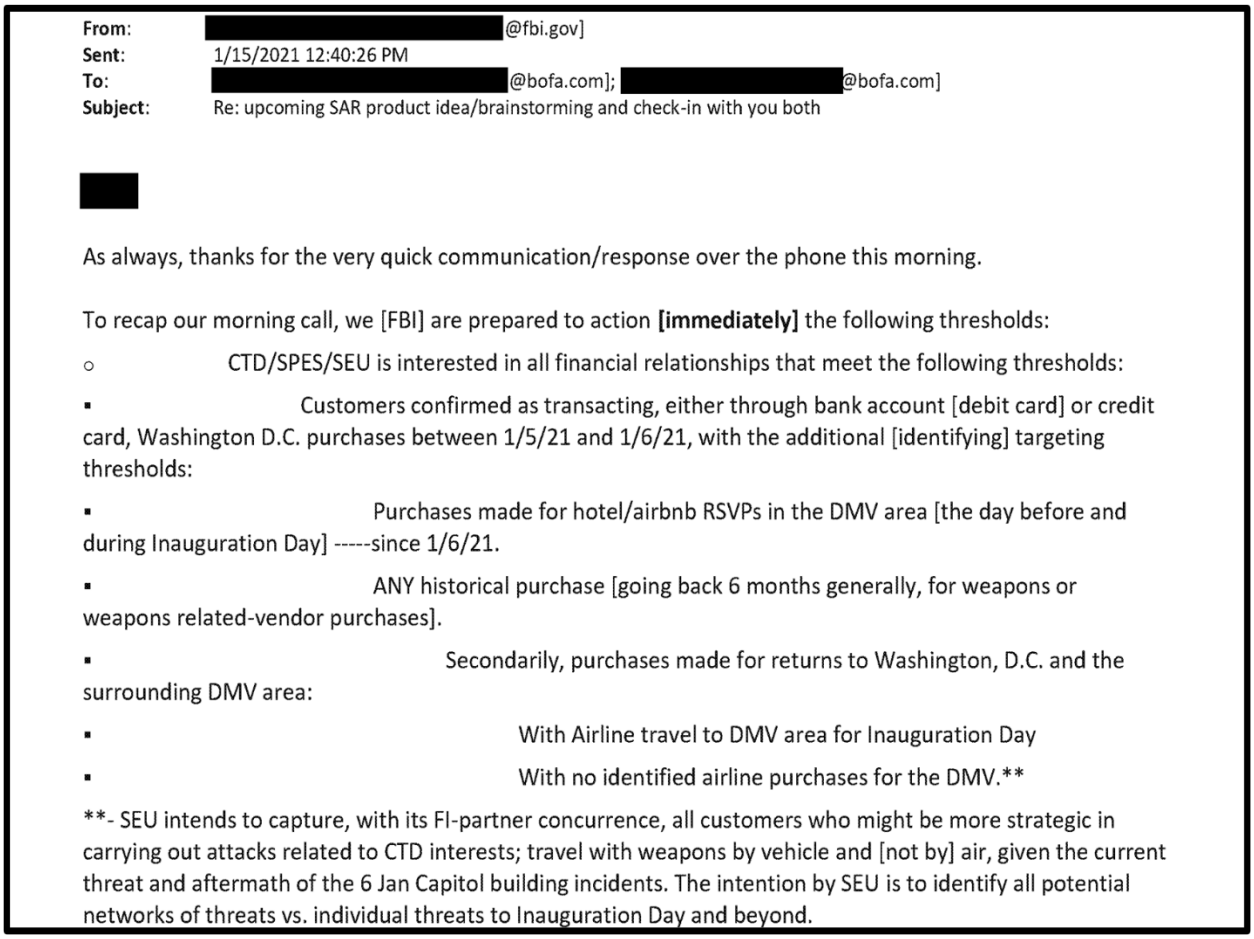
Federal law enforcement has regularly abused the information sharing process in order to deploy financial institutions as *de facto* arms of federal law enforcement. For example, following the events of January 6, 2021, federal law enforcement and FinCEN deputized the entire financial sector to identify anyone who may have been present at the U.S. Capitol.[135] This collaboration included sharing information and developing typologies that clearly targeted Americans with conservative views—gun owners, those concerned with illegal immigration, and those opposed to COVID mandates, to name a few.[136] The FBI exploited its relationships with financial institutions by asking them to file SARs based on specific typologies crafted by FinCEN and the FBI to ostensibly identify potential threats to Inauguration Day.[137] Yet, even after Inauguration Day had concluded and any potential threats to the event had passed, the FBI still sent financial institutions specific names, requesting that they search their database for those individuals and file SARs on any potential suspicious activity.[138]

On January 8, 2021, FinCEN convened a call with Peter Sullivan, representing the FBI's Counterterrorism Division, and approximately thirty to fifty financial institutions.[139] On this call and others, "FinCEN asked [the FBI] to discuss different fact-based patterns that would help institutions look at their data, review their data for anything . . . that would help the institutions understand if they had any threats . . . ."[140] Following the January 8, 2021, conversation, BoA reached out to Sullivan directly to discuss the FinCEN call.[141] On January 15, 2021, Sullivan and BoA representatives "brainstorm[ed]" potential indicators and thresholds that could be used by BoA to file a SAR related to the events at the Capitol on January 6, 2021, and to identify potential threats to Inauguration Day.[142] Sullivan memorialized this call in an email to BoA with

---

[134] *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN PENALIZES U.S. BANK OFFICIAL FOR CORPORATE ANTI-MONEY LAUNDERING FAILURES (Mar. 4, 2020) (noting that FinCEN assessed $450,000 civil penalty against U.S. Bank Official for "failure to prevent violations of the Bank Secrecy Act" and $185 million civil penalty against U.S. Bank for "willfully violating the BSA's requirements").
[135] *See* Transcribed Interview of Mr. Peter Sullivan at 66-67 (Apr. 9, 2024); *see also* Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002) (including thresholds confirming customers transacting in Washington, D.C. or purchasing hotel reservations in Washington, D.C.).
[136] *See* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 17 (Comm. Print 2024).
[137] *See* Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002); *see also* Transcribed Interview of Mr. Peter Sullivan at 29 (Apr. 9, 2024) (Sullivan testified that the FBI shared "fact-based patterns" with financial institutions to "help the institutions understand if they had any threats that may help cover down on the threat to Inauguration Day").
[138] *See, e.g.*, Email from Peter Sullivan, FBI, to FBI employee and Bcc'd recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084); Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Jan. 15, 2021, 10:25 AM) (SCB-00002713).
[139] Transcribed Interview of Mr. Peter Sullivan at 27, 29, 80, 92 (Apr. 9, 2024) (noting that the FinCEN call occurred on January 8, 2021).
[140] *Id.* at 29.
[141] *Id.* at 28.
[142] *Id.* at 28-30.

a list of thresholds the FBI was "prepared to action."[143] According to these thresholds, the FBI sought information on any BoA customer who transacted in the Washington, D.C., area and who made "ANY historical purchase" of a firearm or who had made a hotel, Airbnb, or airline reservation within a given date range in January 2021.[144]



From: [redacted]@fbi.gov]
Sent: 1/15/2021 12:40:26 PM
To: [redacted]@bofa.com]; [redacted]@bofa.com]
Subject: Re: upcoming SAR product idea/brainstorming and check-in with you both

[redacted]

As always, thanks for the very quick communication/response over the phone this morning.

To recap our morning call, we [FBI] are prepared to action **[immediately]** the following thresholds:

- CTD/SPES/SEU is interested in all financial relationships that meet the following thresholds:
  - Customers confirmed as transacting, either through bank account [debit card] or credit card, Washington D.C. purchases between 1/5/21 and 1/6/21, with the additional [identifying] targeting thresholds:
    - Purchases made for hotel/airbnb RSVPs in the DMV area [the day before and during Inauguration Day] -----since 1/6/21.
    - ANY historical purchase [going back 6 months generally, for weapons or weapons related-vendor purchases].
    - Secondarily, purchases made for returns to Washington, D.C. and the surrounding DMV area:
      - With Airline travel to DMV area for Inauguration Day
      - With no identified airline purchases for the DMV.**

**- SEU intends to capture, with its FI-partner concurrence, all customers who might be more strategic in carrying out attacks related to CTD interests; travel with weapons by vehicle and [not by] air, given the current threat and aftermath of the 6 Jan Capitol building incidents. The intention by SEU is to identify all potential networks of threats vs. individual threats to Inauguration Day and beyond.

*"[W]e [FBI] are prepared to action **[immediately]** the following thresholds . . . Washington D.C. purchases between 1/5/21 and 1/6/21 . . . [p]urchases made for hotel/Airbnb RSVPs in the DMV area . . . ANY historical purchase [going back 6 months generally, for weapons or weapons related-vendor purchases] . . . ."*
—Jan. 15, 2021, email from FBI personnel to Bank of America personnel

Ultimately, according to Sullivan, BoA filed a SAR based on these FBI-provided thresholds. Sullivan testified:

> Q. And did Bank of America's production of the SAR and information that was in the SAR, did it correlate with these thresholds?

[143] Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002).
[144] *Id.*

A. It did.

* * *

Q. Do you recall how many individuals then were identified in that SAR?

A. My recollection is that there were 211 individuals that met the three thresholds that you can see within the email.[145]

Sullivan's interactions, however, were not limited to only BoA. He testified that, "my engagement was not just with Bank of America. My engagement was with all [of the] finance sector. And so that covered banks, fintech, it covered neobanks, cryptocurrency, I mean, you name it."[146] Sullivan stated that "a handful" of those financial institutions, like BoA, filed SARs based on thresholds developed by the FBI and FinCEN and that, at times, he even received SARs that were "handpicked" for him directly by executives at financial institutions.[147] He testified:

Q. Do you know, approximately, how many other banks . . . did, in fact, send you information complying with those three criteria like Bank of America did[?]

A. Yeah, there were between 40 and 60 representatives on the first FinCEN [call], which probably spanned 30 to 50 financial institutions. So I received a lot of SARs related to the Capitol riots and the unknown threat to Inauguration Day.[148]

Following the January 8 phone call between FinCEN, the FBI, and financial institutions, FinCEN "created a tag for all SARs related to the Capitol riots"[149] and financial institutions swiftly complied with FinCEN's and the FBI's requests, directing their employees to expedite SARs related to the events of January 6, 2021.[150] In an email from a Citigroup Senior Vice President, employees received direction that "for any SAR filings related to the Capitol Riots, the following reference should be included in SAR Field 2 (Filing Institution Note to FinCEN) and in the narrative of the SAR: '**FIN-2021-DE01**.'"[151] It further directed, "[a]s a reminder, all SARs related to the Capitol Riots should be **expedited**."[152]

---

[145] Transcribed Interview of Mr. Peter Sullivan at 34 (Apr. 9, 2024).
[146] *Id.* at 31-32.
[147] *Id.* at 22, 80.
[148] *Id.* at 80.
[149] *Id.* at 77-78.
[150] *Id.* at 91; *see also* Email from personnel at Citigroup to personnel at Citigroup (Jan. 15, 2021, 4:10 PM) (HJCSWFG_0000648).
[151] Email from personnel at Citigroup to personnel at Citigroup (Jan. 15, 2021, 4:10 PM) (HJCSWFG_0000648) (emphasis in original).
[152] *Id.* (emphasis in original).

Despite stating that the SAR filing process was voluntary, Sullivan could not recall a single financial institution that declined to produce a SAR after the FBI sent the thresholds for banks to use in compiling SARs. Sullivan testified:

> Q. [I]s it voluntary for Bank of America to file a SAR after discussing the very thresholds that were subsequently filed by Bank of America with you?
>
> A. Under BSA, it would be up to the bank exclusively whether or not they met [the] SAR thresholds[.]
>
> Q. Anyone not respond? . . . Any financial institutions you sent similar requests to, like you did [with] Bank of America, and Bank of America sent you back information, including documentation that included 211 American customer names, any other financial institutions you sent similar stuff to, did they not respond?
>
> * * *
>
> A. I can't recall any financial institution that didn't produce SARs during that time.[153]

While the FBI frequently claims that financial institutions voluntarily produce SARs, this information raises questions about whether financial institutions truly have a choice to file SARs when the FBI solicits them.

Ultimately, the FBI's focus shifted from sending thresholds and typologies to financial institutions to soliciting information on specific individuals potentially under investigation.[154] On January 15, 2021, Sullivan sent an email to various financial institutions with the subject line "[a]dditional names/selectors for SAR purposes only at your [financial institution's] discretion."[155] The email included names and other selectors "linked to the 6 Jan Capitol building incidents . . . for SARs purposes only."[156] In other words, Sullivan, on behalf of the FBI, provided a list of Americans to financial institutions suggesting that the companies search their databases to find additional information and potentially file SARs on those individuals.

---

[153] Transcribed Interview of Mr. Peter Sullivan at 90-91 (Apr. 9, 2024).
[154] *See, e.g.*, Email exchange between Peter Sullivan at FBI, FBI employee, personnel at Union Bank and MUFG (Apr. 16, 2021) (MUFG-0000075-76).
[155] Email from Peter Sullivan, FBI, to FBI employee and bcc'd recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084); *see also* Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Jan. 15, 2021, 10:25 AM) (SCB-00002713-2714) (similarly providing names and selectors).
[156] Email from Peter Sullivan, FBI, to FBI employee and bcc'd recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084).

#External Sender# Additional names/selectors for SAR purposes only at your FI's discretion

From:	[redacted] (CTD) (FBI)" [redacted]@fbi.gov>
To:	[redacted] (CTD) (FBI)" [redacted]@fbi.gov>
Bcc:	[redacted]" <[redacted]@santander.us>
Date:	Fri, 15 Jan 2021 15:25:25 +0000
Attachments:	List of names and selectors for SAR purposes only.docx (25.37 kB)

Folks,

SEU has been working hard over the last week to get you additional names/selectors linked to the 6 January Capitol incident and the current threat environment leading up to Inauguration Day.

Please see the attached list of names/selectors linked to the 6 Jan Capitol building incidents and review at the discretion of your own investigation/compliance teams---**for SARs purposes only.**

If you chose to publish a SAR, SEU will be interested to review and disseminate to the appropriate FBI operations personnel immediately.

To be clear, none of the names on this list are part of our SEU's code Yellow/Red/Equity Check outreach tool. But this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course of value-added SAR production.

SEU requests that nothing in the attached be considered a higher priority than SEU's current [pending and future] outreach code YELLOWs/REDs/Equity Checks.

[redacted]

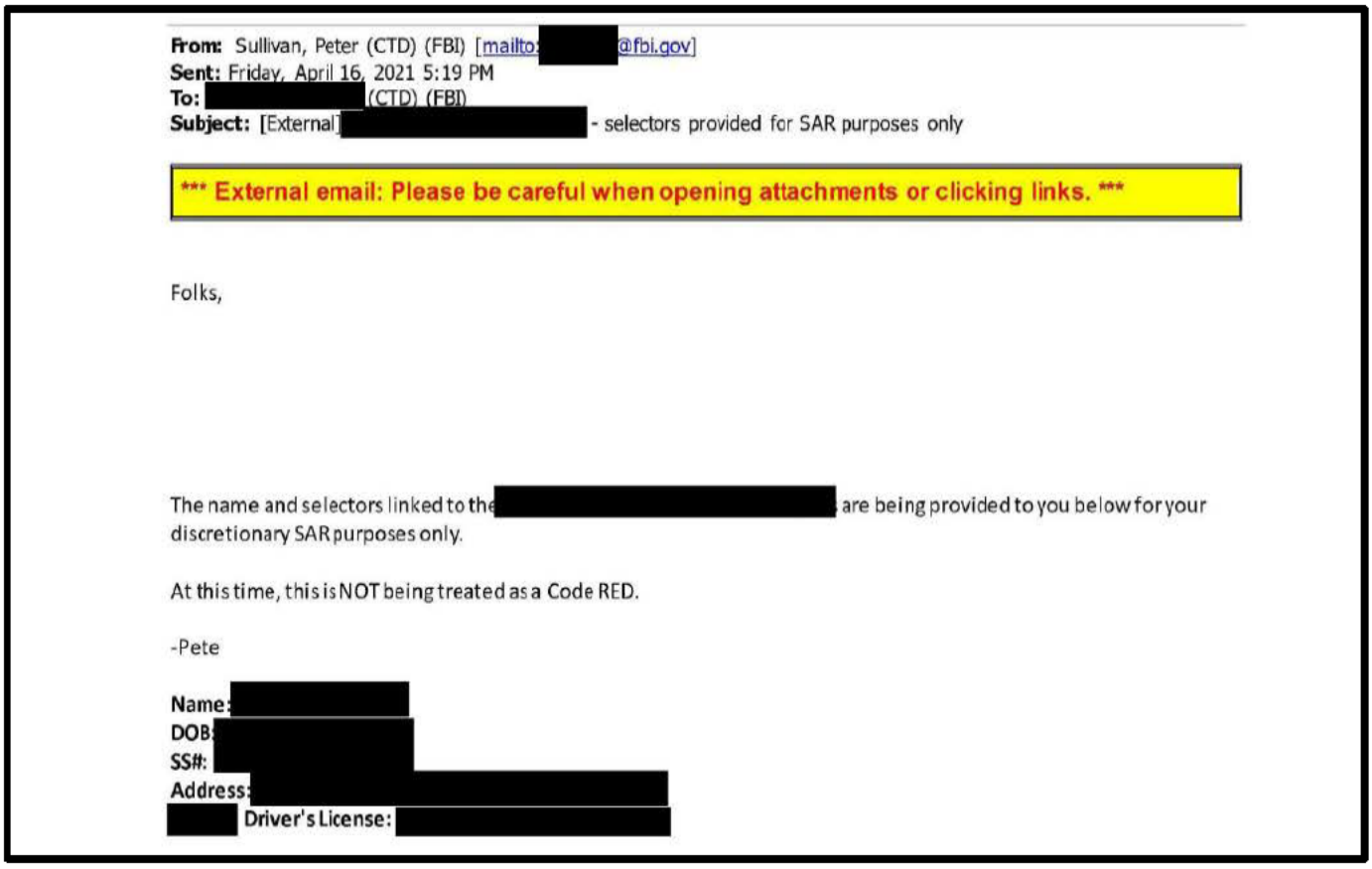
[redacted]
Senior Private Sector Partner Outreach
Strategic Partner Engagement Section
desk: 202-324-2990
cell: 202-570-6825

"SEU has been working hard over the last week to get you additional names/selectors . . . this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course of value-added SAR production."
—Jan. 15, 2021, email from Peter Sullivan, FBI, to FBI employee, and bcc'd financial institutions

However, despite Sullivan's assurance to financial institutions that his information sharing was a part of the "normal course of value-added SAR production,"[157] the FBI's provision of specific names and selectors was a manipulation of the SAR-filing process, which "requires that a *bank or other financial institution* file a SAR whenever *it* identifies 'a suspicious transaction relevant to a possible violation of law or regulation.'"[158] Indeed, as Deputy Director Kirby testified in his transcribed interview, "[W]ith a suspicious activity report it's the bank who's investigating or monitoring their customers and then flagging for FinCEN and law enforcement what they deem to be suspicious."[159] By sending specific names to financial institutions and requesting any SARs related to those individuals, however, the FBI is turning the SAR process on its head, suggesting for the banks that certain people could be suspicious and impliedly urging financial institutions to examine them more closely.

[157] *Id.*
[158] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (emphasis added).
[159] Transcribed Interview of Mr. Jimmy Kirby at 98-99 (July 18, 2024).

In a similar exchange months later, on April 16, 2021, Sullivan shared with various financial institutions a "name and selectors . . . for your discretionary SAR purposes only."[160] In response, an MUFG employee asked "[d]oes this mean you are not looking for a response from us except to notify you if we happen to file something based on this?"[161] Sullivan replied that the FBI "will take any SARs you decide to file on."[162] In his transcribed interview, Sullivan explained that he received, on behalf of the FBI, "a hundred SARs" each year that are "handpicked" directly "from an executive at a financial institution."[163]



From: Sullivan, Peter (CTD) (FBI) [mailto: [redacted]@fbi.gov]
Sent: Friday, April 16, 2021 5:19 PM
To: [redacted] (CTD) (FBI)
Subject: [External] [redacted] - selectors provided for SAR purposes only

*** External email: Please be careful when opening attachments or clicking links. ***

Folks,

The name and selectors linked to the [redacted] are being provided to you below for your discretionary SAR purposes only.

At this time, this is NOT being treated as a Code RED.

-Pete

Name: [redacted]
DOB: [redacted]
SS#: [redacted]
Address: [redacted]
[redacted] **Driver's License:** [redacted]

"[S]electors . . . are being provided to you below for your discretionary SAR purposes only . . . this is NOT being treated as a Code RED."
—Email from Peter Sullivan, FBI, to bcc'd financial institutions

[160] Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Apr. 16, 2021, 5:19 PM) (MUFG-0000075-76).
[161] Email from personnel at MUFG to Peter Sullivan, FBI, FBI employee, and personnel at Union Bank (Apr. 16, 2021 5:46 PM) (MUFG-0000075-76).
[162] Email from Peter Sullivan, FBI, to personnel at MUFG, Union Bank, and FBI employee (Apr. 16, 2021, 9:55 PM) (MUFG-0000075).
[163] *See* Transcribed Interview of Mr. Peter Sullivan at 21-22 (Apr. 9, 2024).

Message

From: [redacted](CTD) (FBI)[redacted]@fbi.gov]
Sent: 4/16/2021 9:55:51 PM
To: [redacted][/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7[redacted]; [redacted](CTD) (FBI) [redacted]@fbi.gov]
CC: [redacted][/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]unionbank.com]; [redacted] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]unionbank.com]; [redacted] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN[redacted].unionbank.com]
Subject: [External] RE:[redacted] selectors provided for SAR purposes only

***** External email: Please be careful when opening attachments or clicking links. *****

[redacted]

This may turn into a code red, but in the interim we wanted to push you selectors we confirmed on the ops side. So yes, for now, we have not confirmed we have GJS' teed up for all results from our normal "code red" protocol --but we will take any SARs you decide to file on.

If this turns into a code red over the weekend, you will hear it from me first.

Hope this helps.

Hope you all have a safe weekend with your families.

[redacted]

From: [redacted]@us.mufg.jp>
Sent: Friday, April 16, 2021 5:46 PM
To: [redacted](CTD) (FBI) [redacted]@fbi.gov>; [redacted](CTD) (FBI) [redacted]@fbi.gov>
Cc: [redacted]@unionbank.com>; [redacted]@unionbank.com>; [redacted]@unionbank.com>
Subject: [EXTERNAL EMAIL] - RE:[redacted] - selectors provided for SAR purposes only

Hi [redacted], happy Friday. Does this mean you are not looking for a response from us except to notify you if we happen to file something based on this?

From: [redacted](CTD) (FBI) [redacted]@fbi.gov]
Sent: Friday, April 16, 2021 5:19 PM
To: [redacted](CTD) (FBI)
Subject: [External][redacted] - selectors provided for SAR purposes only

***** External email: Please be careful when opening attachments or clicking links. *****

Folks,

"We will take any SARs you decide to file on."
—Apr. 16, 2021, Email from Peter Sullivan, FBI, to Union Bank personnel

In at least two instances, one financial institution replied to Sullivan's emails and sought legal process from the FBI before it would turnover more detailed financial records. Sullivan pushed back on those requests. On April 20, 2021, Sullivan sent an email to Standard Chartered employees, requesting information on various names "in response to a **CODE YELLOW**."[164] Standard Chartered responded to Sullivan and informed him that its search registered a "positive hit" but stated that "[i]f additional information is required, we ask that you send a subpoena."[165] Sullivan responded, asking for a phone call, explaining that "typically for Code Reds and Yellows, we get more on the front end than 'positive' only" and affirmed that "because this outreach name on [redacted] was a code yellow, we'd like to get something additional."[166] He contrasted this request with "Equity Checks" that require a response of "'positive' only with no other info offered because Equity Checks are priority investigations but have no . . . emergency-related nexus."[167]

In a similar exchange, on May 24, 2021, Sullivan requested that Standard Chartered "run the following name and associated selectors in response to an Equity Check."[168] Standard Chartered responded, acknowledging that it had identified transactions "with an exact name match," but again asked for legal process, writing, "If additional information is required, we ask that you send a subpoena."[169] Two days later, on May 26, 2021, Sullivan replied to Standard Chartered asking, "I wanted to revisit our conversation on your two cents if we could discuss next steps to try to get more information on name matches . . . ."[170] Sullivan and the Standard Chartered employee scheduled a call for the next day.[171] Sullivan also sought a "pre-call" with the Standard Chartered employee to see if the bank planned to have "compliance or someone else on the call" so that Sullivan could "make sure at a minimum" that he was on "the same page" as the Standard Chartered employee regarding these requests.[172] This apparent effort to avoid any legal process to obtain the sensitive information of a bank's customer is concerning, but does not appear uncommon.

The FBI clearly recognizes the usefulness of Americans' financial data and frequently contacts financial institutions to request information for the FBI's investigations. While avoiding making outright demands for this information, documents show that the FBI avoids requests for legal process and routinely operates on the edge of what is permissible information sharing under

---

[164] Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Apr. 19, 2021, 5:43 PM) (SCB-00002923) (emphasis in original).
[165] Email from personnel at Standard Chartered Bank to Peter Sullivan at FBI, FBI employee, and personnel at Standard Chartered Bank (Apr. 20, 2021, 2:52 PM) (SCB-00002923).
[166] Email from Peter Sullivan, FBI, to personnel at Standard Chartered Bank and FBI employee (Apr. 20, 2021, 4:46 PM) (SCB-00002922).
[167] *Id.*
[168] Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (May 24, 2021, 11:58 AM) (SCB-00003013).
[169] Email from personnel at Standard Chartered Bank to Peter Sullivan, FBI, FBI employee, and personnel at Standard Chartered Bank (May 24, 2021, 4:04 PM) (SCB-00003012).
[170] Email exchange between Peter Sullivan, FBI, to personnel at Standard Chartered Bank (May 26, 2021) (SCB-00003012).
[171] Email from personnel at Standard Chartered Bank to Peter Sullivan, FBI (May 26, 2021, 3:40 PM) (SCB-00003018).
[172] Email from Peter Sullivan, FBI, to personnel at Standard Chartered Bank (May 26, 2021, 8:19 PM) SCB-00003018).

the BSA. By soliciting financial institutions for SAR filings directly, the FBI is treating financial institutions as arms of law enforcement charged with investigating whether a customer has engaged in any "suspicious activity" on the FBI's behalf.

B. FinCEN solicits customer transaction information from financial institutions, on behalf of the FBI, even if the transaction activity lacks a clear nexus to criminal activity.

FinCEN also serves as an active partner of the FBI by collecting Americans' financial data on its behalf. During his transcribed interview, the former Director of the Office of Stakeholder Integration and Engagement in the Strategic Operations Division at FinCEN, stated that "if the FBI said, hey, we're desperate; you know, something major is happening . . . we need you to jump, we would jump."[173] This closeness played out following January 6, 2021, when FinCEN coordinated with the FBI to share hordes of information with financial institutions to assist in the FBI's investigation. The Committee and Select Subcommittee's investigation has revealed that FinCEN provided financial institutions with politicized search terms and typologies that cast certain ideologies, namely conservatives, as potentially dangerous or extreme.[174] New documents reveal that, as it sought to assist the FBI in its January 6-related investigations, FinCEN cast such a wide net that it inevitably caused financial institutions to flag ordinary Americans' transactions as suspicious.

One example that demonstrates the problem with casting such a wide net, is a list that FinCEN circulated to financial institutions that included hundreds of shops and vendors that any traveler would have made at D.C.-area airports, train stations, and bus stops, including purchases from major nationwide food and retail chains.[175] On January 22, 2021, after the presidential inauguration, an employee from MUFG sent FinCEN an email with an excel sheet that included "a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops."[176] A FinCEN employee responded to MUFG, saying, "this is terrific. Thank you both."[177]

---

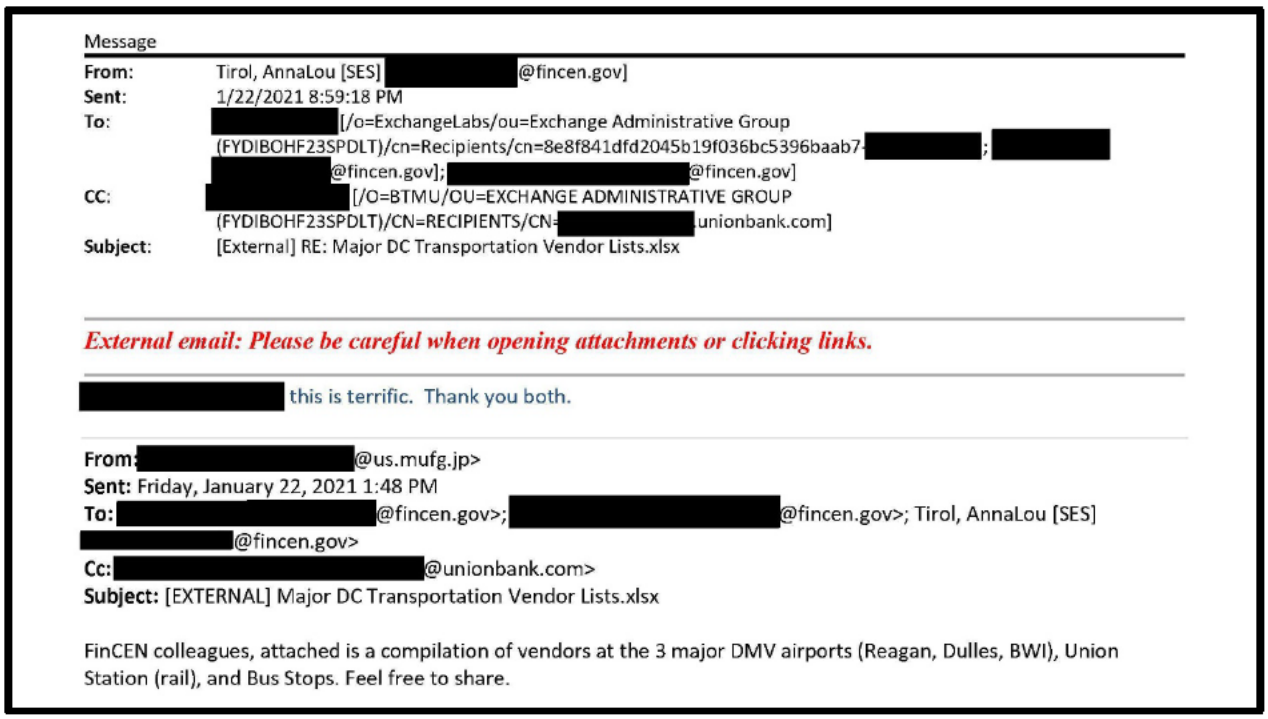
[173] Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 21-22 (May 14, 2024).

[174] *See* STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 21-22 (Comm. Print 2024).

[175] List of airport and bus stop vendors in the Washington, D.C. area (MUFG-0000417.XLSX).

[176] Email from personnel at MUFG to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, FinCEN employee, and AnnaLou Tirol, FinCEN, and personnel at Union Bank (Jan. 22, 2021 1:48 PM) (MUFG-0000806).

[177] Email from AnnaLou Tirol, FinCEN, to personnel at MUFG, the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, FinCEN employee, and personnel at Union Bank (Jan. 22, 2021 8:59 PM) (MUFG-0000806).



Message

From: Tirol, AnnaLou [SES] [redacted]@fincen.gov]
Sent: 1/22/2021 8:59:18 PM
To: [redacted][/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7-[redacted]; [redacted]@fincen.gov]; [redacted]@fincen.gov]
CC: [redacted][/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted].unionbank.com]
Subject: [External] RE: Major DC Transportation Vendor Lists.xlsx

External email: Please be careful when opening attachments or clicking links.

[redacted] this is terrific. Thank you both.

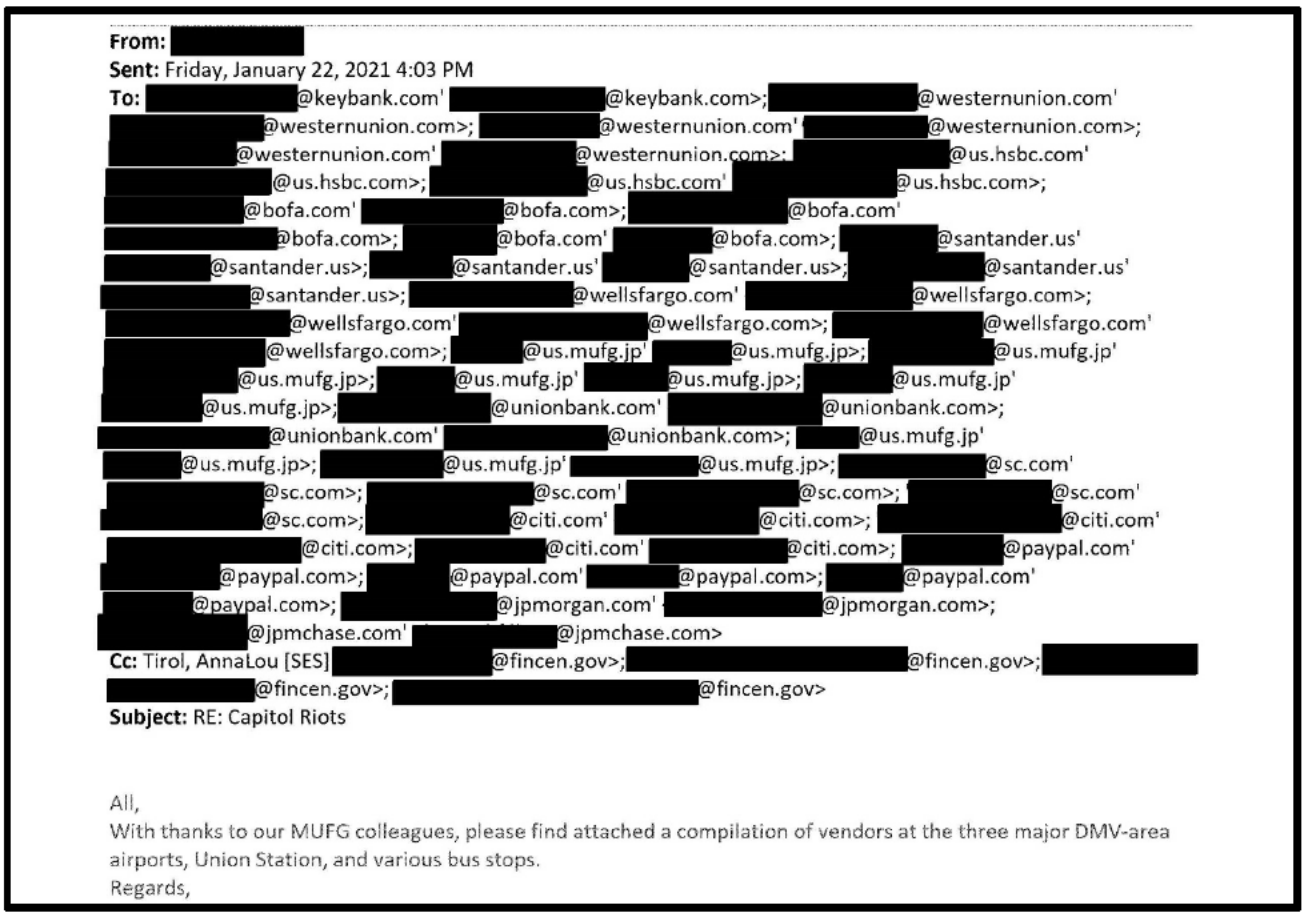
From: [redacted]@us.mufg.jp>
Sent: Friday, January 22, 2021 1:48 PM
To: [redacted]@fincen.gov>; [redacted]@fincen.gov>; Tirol, AnnaLou [SES] [redacted]@fincen.gov>
Cc: [redacted]@unionbank.com>
Subject: [EXTERNAL] Major DC Transportation Vendor Lists.xlsx

FinCEN colleagues, attached is a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops. Feel free to share.

"[A]ttached is a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops. Feel free to share."
—Email from MUFG personnel to FinCEN personnel

FinCEN shared this compilation of vendors with financial institutions.[178]

[178] Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to personnel at KeyBank, Western Union, HSBC, Bank of America, Santander, Wells Fargo, MUFG, Union Bank, MUFG, Standard Chartered Bank, Citibank, PayPal, JPMorgan Chase, and AnnaLou Tirol at FinCEN, and FinCEN personnel (Jan. 22, 2021 4:03 PM) (WesternUnion-0000646).



From: [redacted]
Sent: Friday, January 22, 2021 4:03 PM
To: [redacted]@keybank.com' [redacted]@keybank.com>; [redacted]@westernunion.com' [redacted]@westernunion.com>; [redacted]@westernunion.com' [redacted]@westernunion.com>; [redacted]@westernunion.com' [redacted]@westernunion.com>; [redacted]@us.hsbc.com' [redacted]@us.hsbc.com>; [redacted]@us.hsbc.com' [redacted]@us.hsbc.com>; [redacted]@bofa.com' [redacted]@bofa.com>; [redacted]@bofa.com' [redacted]@bofa.com>; [redacted]@bofa.com' [redacted]@bofa.com>; [redacted]@santander.us' [redacted]@santander.us>; [redacted]@santander.us' [redacted]@santander.us>; [redacted]@santander.us' [redacted]@santander.us>; [redacted]@wellsfargo.com' [redacted]@wellsfargo.com>; [redacted]@wellsfargo.com' [redacted]@wellsfargo.com>; [redacted]@wellsfargo.com' [redacted]@wellsfargo.com>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@unionbank.com' [redacted]@unionbank.com>; [redacted]@unionbank.com' [redacted]@unionbank.com>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@us.mufg.jp' [redacted]@us.mufg.jp>; [redacted]@sc.com' [redacted]@sc.com>; [redacted]@sc.com' [redacted]@sc.com>; [redacted]@sc.com' [redacted]@sc.com>; [redacted]@citi.com' [redacted]@citi.com>; [redacted]@citi.com' [redacted]@citi.com>; [redacted]@citi.com' [redacted]@citi.com>; [redacted]@paypal.com' [redacted]@paypal.com>; [redacted]@paypal.com' [redacted]@paypal.com>; [redacted]@paypal.com' [redacted]@paypal.com>; [redacted]@jpmorgan.com' [redacted]@jpmorgan.com>; [redacted]@jpmchase.com' [redacted]@jpmchase.com>
Cc: Tirol, AnnaLou [SES] [redacted]@fincen.gov>; [redacted]@fincen.gov>; [redacted]@fincen.gov>; [redacted]@fincen.gov>
Subject: RE: Capitol Riots

All,
With thanks to our MUFG colleagues, please find attached a compilation of vendors at the three major DMV-area airports, Union Station, and various bus stops.
Regards,

"With thanks to our MUFG colleagues, please find attached a compilation of vendors at the three major DMV-area airports, Union Station, and various bus stops."
—Jan. 22, 2021, Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to financial institutions and FinCEN personnel

In his transcribed interview, the former Director of the Office of Stakeholder Integration and Engagement stated that FinCEN shares typologies or red flags with financial institutions to provide guidance for their AML/CFT programs.[179] Therefore, by sharing a compilation of vendors at the major Washington, D.C. area transit facilities, it appears that FinCEN expected banks to use the list to identify people or transactions made at those vendors that may be suspicious and merit a SAR filing. This dragnet, suspicious treatment of purchases at vendors around the DMV area, coincided with the FBI soliciting BoA to search its database for any individuals seeking to travel to the Washington, D.C. area around January 6, 2021, and January 20, 2021, and FinCEN's distribution of a PowerPoint slideshow explaining how financial institutions could search through Americans' transactions using MCC codes and other keywords

[179] Transcribed Interview of former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 50 (May 14, 2024).

like "Bass Pro Shop" and "Dick's Sporting Goods" to scrutinize their purchases.[180] These kinds of sprawling requests have an extremely limited nexus, if any, to individualized criminal conduct. Despite the lack of a criminal nexus, the Treasury Department acknowledged in a letter to the Committee that FinCEN was sharing this kind of information with financial institutions for them to "consider incorporating into their existing AML/CFT programs."[181]

Documents obtained by the Committee and Select Subcommittee indicate that federal law enforcement was not the only entity that was abusing the information-sharing process. Deployed as arms of law enforcement, financial institutions seemingly assumed their role and sought ways to manipulate FinCEN's existing authorities in order to expand the amount of financial data that could be turned over to the FBI.

As an email between MUFG and FinCEN shows, MUFG suggested using the USA PATRIOT Act's Section 314(a) process to notify other financial institutions about what would otherwise be confidential SAR information. The 314(a) process gives investigators the ability "to canvas the nation's financial institutions for potential lead information" from "more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering."[182] MUFG suggested to FinCEN that it should issue 314(a) requests, based on SAR filings, in order to trigger other financial institutions into conducting a review of their databases for any positive matches and presumably file SARs with law enforcement, "assuming [FinCEN has] the authority."[183] But, according to FinCEN, "Section 314(a) provides lead information only and is not a substitute for a subpoena or other legal process."[184] As Deputy Director Kirby testified, this process is "essentially a hand-raising exercise for whether [the financial institutions] have responsive accounts" in response to a law enforcement inquiry, but the response "does not include the actual financial records."[185] Yet, the strategy concocted by MUFG would appear to be a substitute for the Section 314(b) legal process, which already exists so that "financial institutions . . . [can] share information with one another in order to identify and report . . . money laundering or terrorist activity" after notifying the Treasury Department.[186] Though Section 314(b) allows financial institutions to share information with one another, according to FinCEN, the 314(b) process "does not relax the prohibition against SAR disclosures" and financial institutions "remain prohibited from disclosing a SAR or any information that would reveal the existence of a SAR notwithstanding

[180] *See* Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002); *see also* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 27 (Comm. Print 2024).
[181] Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3-4 (Feb. 9, 2024); As the Treasury Department makes clear, "FinCEN and banks shared information about methodologies that banks could consider using as part of their AML/CFT programs to identify indicia of suspicious activity relevant to the January 6 attack on the Capitol or threats of violence in connection with the then-upcoming presidential inauguration." *Id.* at 3-4.
[182] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN'S 314(A) FACT SHEET.
[183] Email exchange between AnnaLou Tirol, FinCEN, and personnel at MUFG (Jan. 14, 2021) (MUFG-0000248-249).
[184] FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN'S 314(A) FACT SHEET.
[185] Transcribed Interview of Mr. Jimmy Kirby at 98 (July 18, 2024).
[186] FINANCIAL CRIMES ENFORCEMENT NETWORK, SECTION 314(B).

Section 314(b)."[187] MUFG apparently proposed the "idea" to "support the Bureau's efforts to address the acute threat of domestic terrorism."[188]

From: Tirol, AnnaLou [SES] [redacted]@fincen.gov]
Sent: 1/14/2021 4:23:40 PM
To: [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7-[redacted]]
Subject: [External] RE: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Terrific - I'll call you at 1. Thanks!

-----Original Message-----
From: [redacted]@us.mufg.jp>
Sent: Thursday, January 14, 2021 11:10 AM
To: Tirol, AnnaLou [SES] [redacted]@fincen.gov>
Subject: [EXTERNAL] RE: Bouncing an Idea off You

Terrific. If you're able to give me a time, just shoot me an email and I'll re-arrange meetings to be available. I'm free right now from 1-2 but as I said, can shift stuff around if need be.

-----Original Message-----
From: Tirol, AnnaLou [SES] [redacted]@fincen.gov]
Sent: Thursday, January 14, 2021 8:34 AM
To: [redacted]
Subject: [External] Re: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Hi [redacted]
It's great to hear from you, and thank you for reaching out with this interesting idea. I will give you a call to chat more, hopefully around midday. I look forward to talking more.
I hope you are safe and well,
AnnaLou

From: [redacted]@us.mufg.jp<mailto:[redacted]@us.mufg.jp>>
Date: Wednesday, January 13, 2021 at 6:41:53 PM
To: "Tirol, AnnaLou [SES]" [redacted]@fincen.gov<mailto:[redacted]@fincen.gov>>
Subject: [EXTERNAL] Bouncing an Idea off You

Confidential

AnaLou, I hope you are well. We live in interesting times. As you might imagine, our bank, and I expect many others, are thinking hard about how we can support the Bureau's efforts to address the acute threat of domestic terrorism we are facing at the moment.

I wanted to bounce an idea off you. Would FinCEN have an appetite (assuming you feel you have the authority) to, in SARs filed in relation to the current acute threat of domestic terrorism, identify whether the suspicious activity being reported involves a customer of another institution in the U.S. and, if so, make a 314(a) request, perhaps under a specific code, for such subjects? In other words, Bank A files a SAR for suspicious transactions involving John Doe, a Customer of Bank B (an FI in the US). However, Bank B is unaware of the concern surrounding its customer (unless Bank A utilized 314(b) authorities–but even then, the delay would be unworkable when addressing an acute terror threat). FinCEN, by doing a 314(a) request for that subject, will trigger an internal review in Bank B (most banks will open an investigation following a 314(a) match). If the 314(a) request is coded under a project name, all the better.

I'm happy to explain myself more in a call. [redacted] I'm also curious if FinCEN is planning anything independently (i.e., red flags circular). I'm sure that BSAAG members would be happy to contribute thoughts and ideas that could be shared more broadly – even with other BSAAG members.

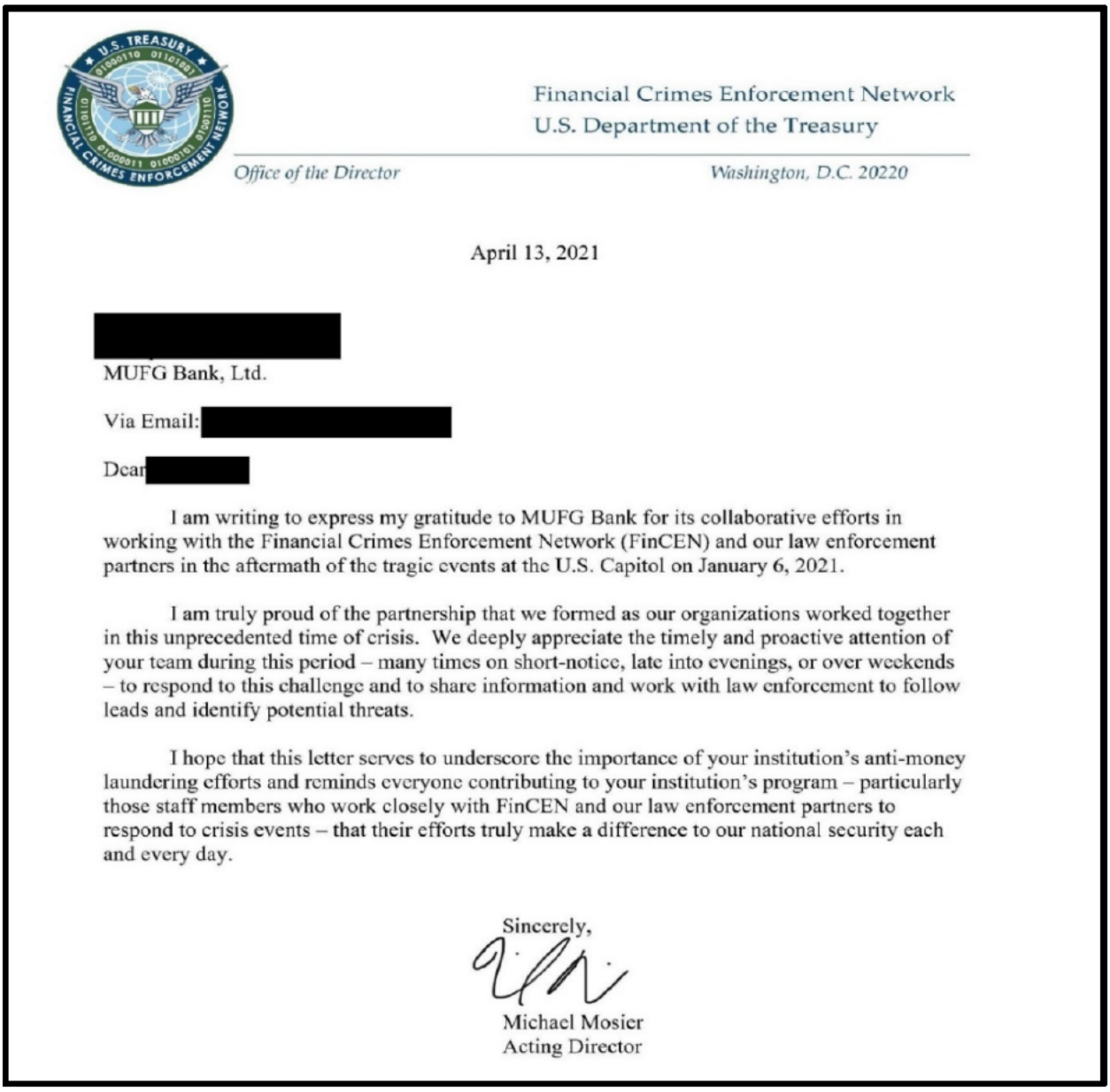
Anyhow, we are open to assisting however we can, within the existing authorities. Take care and say hi to Ken and congratulations to you both on the passage of the NDAA. That's a big accomplishment!

"I wanted to bounce an idea off you. Would FinCEN have an appetite . . . to, in SARs filed in relation to the current acute threat of domestic terrorism, identify whether the suspicious activity being reported involves a customer of another institution in the U.S. and, if so, make a 314(a) request . . . ?"

—Jan. 13, 2021, email exchange between MUFG personnel and AnnaLou Tirol, FinCEN

[187] FINANCIAL CRIMES ENFORCEMENT NETWORK, SECTION 314(B) FACT SHEET.
[188] Email exchange between AnnaLou Tirol, FinCEN, and personnel at MUFG (Jan. 14, 2021) (MUFG-0000248-249).

MUFG's and other financial institutions' efforts to assist FinCEN and federal law enforcement's investigative efforts did not go unnoticed. On April 13, 2021, FinCEN Acting Director Michael Mosier sent a thank you letter to various financial institutions for "the timely and proactive attention of your team during this period – many times on short-notice, late into evenings, or over weekends – to respond to this challenge and to share information and work with law enforcement to follow leads and identify potential threats."[189]



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Office of the Director *Washington, D.C. 20220*

April 13, 2021

[redacted]
MUFG Bank, Ltd.

Via Email: [redacted]

Dear [redacted]

I am writing to express my gratitude to MUFG Bank for its collaborative efforts in working with the Financial Crimes Enforcement Network (FinCEN) and our law enforcement partners in the aftermath of the tragic events at the U.S. Capitol on January 6, 2021.

I am truly proud of the partnership that we formed as our organizations worked together in this unprecedented time of crisis. We deeply appreciate the timely and proactive attention of your team during this period – many times on short-notice, late into evenings, or over weekends – to respond to this challenge and to share information and work with law enforcement to follow leads and identify potential threats.

I hope that this letter serves to underscore the importance of your institution's anti-money laundering efforts and reminds everyone contributing to your institution's program – particularly those staff members who work closely with FinCEN and our law enforcement partners to respond to crisis events – that their efforts truly make a difference to our national security each and every day.

Sincerely,

Michael Mosier
Acting Director

"I am writing to express my gratitude to MUFG Bank for its collaborative efforts in working with [FinCEN] and our law enforcement partners in the aftermath of the tragic events at the U.S. Capitol on January 6, 2021 . . . I am truly proud of the partnership that we formed . . . ."
—Apr. 13, 2021, Michael Mosier, FinCEN, to MUFG personnel

[189] Michael Mosier, FinCEN, to personnel at MUFG, Apr. 13, 2021 (MUFG-0001196).

This letter exemplifies FinCEN and law enforcement's expectation that financial institutions work to assist the federal government whenever the government calls.

C. The federal government, through the BSAAG advisory group, is increasing its coordination with financial institutions and pushing them to adopt new and invasive technologies that augment the ability to surveil Americans.

Established by the Annunzio-Wylie Anti-Money Laundering Act of 1992,[190] the Bank Secrecy Act Advisory Group (BSAAG) advises the Treasury Department on issues related to the BSA.[191] The BSAAG includes representatives from government agencies like the Treasury and Justice Departments, national financial institutions, trade associations, and other businesses subject to the reporting requirements of the BSA.[192] Documents obtained by the Committee and Select Subcommittee indicate that the federal government, through the BSAAG, is pushing financial institutions to integrate new technologies, such as AI and digital ID requirements, that will expand the access to and surveillance of Americans' data.

i. BSAAG documents indicate that Big Banks and Big Government are advancing the implementation of a national digital ID system.

As the world becomes increasingly digitized, there has been a global push toward requiring digital identification systems.[193] These systems, under the guise of modernizing identity verification, are designed to authenticate a claimed identity with the real-life existence of the individual "us[ing] electronic means to assert and prove a person's official identity online."[194] Traditionally, verifying a person's identity has relied on physical documents like driver's licenses and passports.[195] However, in the United States and around the globe, interest groups comprised of financial institutions, influential global organizations, and various governmental bodies are pushing the integration of a national "digital ID" system into financial and public services.[196] Troublingly, the Committee and Select Subcommittee obtained a confidential BSAAG Working Group White Paper, titled "Brick & Mortar to Bits & Bytes: Adapting the U.S. AML/CFT Regime for Digital Identity," which indicates that a push for a national digital ID requirement in the United States appears to be underway and that financial services may be the vehicle for its adoption.[197]

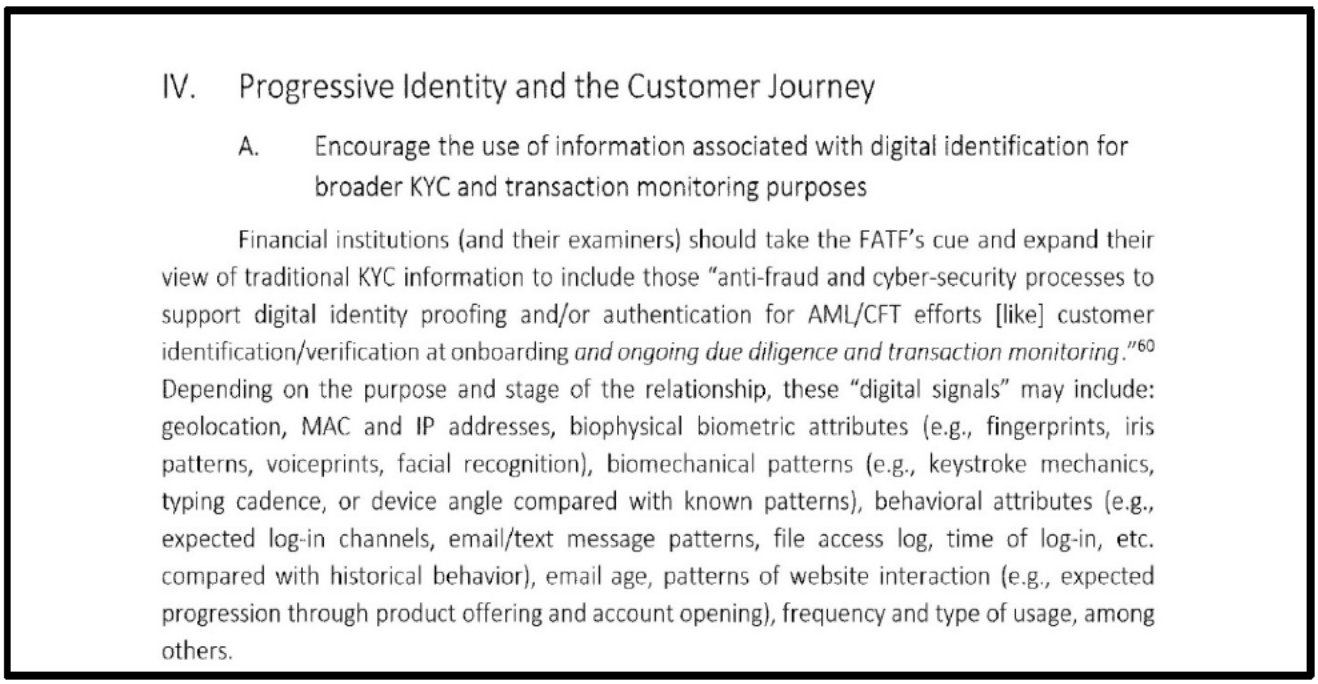
---

[190] Pub. L. No. 102-550, 106 Stat. 3672 (1992).
[191] *See* Bank Secrecy Act Advisory Group; Solicitation of Application for Membership, 88 Fed. Reg. 9329 (Feb. 13, 2023).
[192] CHARTER OF THE BANK SECRECY ACT ADVISORY GROUP, FINCEN.
[193] *See, e.g.*, Ash Johnson, *The Path to Digital Identity in the United States*, Information Technology & Innovation Foundation (Sept. 23, 2024).
[194] Financial Action Task Force, *Guidance on Digital Identity* ¶ 57 (Mar. 2020).
[195] *See id.* at ¶ 109.
[196] *See* Kanwaljit Singh, Digital IDs are an effective tool against poverty, Bill & Melinda Gates Foundation, https://www.gatesfoundation.org/ideas/articles/mosip-digital-id-systems (Aug. 15, 2024); *see also* WORLD BANK, *Digital ID to Enhance Financial Inclusion: A Toolkit for Regulatory Authorities* (Dec. 2021), https://documents1.worldbank.org/curated/en/099650005162214653/pdf/P16477001277440f10b8080dc6f51daf2dc.pdf.
[197] *Brick & Mortar to Bits & Bytes: Adopting the U.S. AML/CFT Regime for Digital Identity*, BSAAG FinTech/RegTech Working Group (SCHWAB_HJC_00000717).

In the white paper, the BSAAG Working Group acknowledged "the reality that there is [a] deep political and cultural skepticism of, or even hostility to, a national ID system in the U.S.," and that the "national ID system will face unique political challenges and structural hurdles in the U.S. . . ."[198] Despite this public skepticism, the BSAAG Working Group recommended that "U.S. financial institutions . . . support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and ongoing due diligence and transaction monitoring) . . . ."[199] The white paper also discussed how the biometric information and digital signals enabled by the use of digital ID could be repurposed for "broader KYC [Know-Your-Customer] and transaction monitoring purposes," mentioning, in particular the use of:

- "geolocation, MAC and IP addresses,"
- "biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition),"
- "biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns),"
- "behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage . . . ."[200]

[198] *Id.*
[199] *Id.* at 00000718-719 (internal quotations omitted).
[200] *Id.* at 00000736.



IV. Progressive Identity and the Customer Journey

A. Encourage the use of information associated with digital identification for broader KYC and transaction monitoring purposes

Financial institutions (and their examiners) should take the FATF's cue and expand their view of traditional KYC information to include those "anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts [like] customer identification/verification at onboarding *and ongoing due diligence and transaction monitoring*."[60] Depending on the purpose and stage of the relationship, these "digital signals" may include: geolocation, MAC and IP addresses, biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition), biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns), behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage, among others.

"Encourage the use of information associated with digital identification for broader [Know-Your-Customer] and transaction monitoring purposes"
—BSAAG FinTech/RegTech Working Group

The white paper also noted that successful digital ID implementation would have "potentially profound policy implications and benefits" by "focusing financial institutions on behavioral risk" and "leveraging the digital signals" financial institutions would gain from digital ID to better surveil its customers for behavior that the bank considers risky.[201] This includes expanding and utilizing a concept called "progressive identity" which "recognizes that digital ID is not simply a new method for static identification and verification, but can facilitate the 'customer journey' through which customers increase their digital footprint . . . ."[202] If digital ID and the concept of "progressive identity" are integrated into American financial regulation, government surveillance is likely to pervade even deeper into Americans' financial activities as the "digital footprint" of Americans increase.

The BSAAG document explicitly stated, "*First,* the U.S. AML regime should create the conditions for digital ID practices to take root in the U.S. financial industry by expanding and updating the existing customer identification program (CIP) rules . . . ."[203] In doing so, digital ID is sold as a portable and secure way of determining the validity of an individual's credentials;[204] however, in reality, digital ID can be a potential Trojan horse. It can be a governmental tool used

[201] *Id.* at 00000720.
[202] *Id.* at 00000720, 736.
[203] *Id.* at 00000719.
[204] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Digital Identity Guidelines: Enrollment and Identity Proofing (2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf; *see also Digital Identity: Why It Matters and Why It's Important We Get It Right*, WORLD ECONOMIC FORUM (Jan. 26, 2018), https://www.weforum.org/press/2018/01/digital-identity-why-it-matters-and-why-it-s-important-we-get-it-right/.

to regulate access to banking services and can lead to constant surveillance, as every transaction becomes associated with a digital ID. Some proponents maintain that individuals will have control over their information and the ability to voluntarily participate in the system, but, in practice, digital ID often becomes mandatory, leaving individuals with no choice but to surrender their privacy.[205]

Indeed, the BSAAG document speaks to the consequences of refusing to comply with digital ID signals, "if a customer uses a VPN [Virtual Private Network] or blocks location permissions—both legitimate privacy-based decisions—the progressive identity of the customer will be hampered . . . as the financial institution may likely have to resort to more traditional KYC [Know-Your-Customer] techniques or *limit the customer's access to its services*."[206] In other words, making "legitimate privacy-based decisions" may result in a different reality: either accept these tools of surveillance and digital ID, or risk being debanked.

ii. The federal government encouraged financial institutions to incorporate new technologies, including artificial intelligence and machine learning, into their systems to more aggressively track Americans.

Incorporating artificial intelligence (AI) and machine learning (ML) into financial institutions' AML programs also appears to be a priority of the BSAAG. In April of 2022, Himamauli Das, the then-Acting Director of FinCEN, testified before the House Committee on Financial Services that "we can envision consideration of efforts involving artificial intelligence or machine learning-driven transaction monitoring . . . digital identity tools . . . and automating the adjudication and filing of SARs related to certain types of activity."[207] Confidential BSAAG documents obtained by the Committee and Select Subcommittee reveal that digital identity tools, along with AI and ML solutions, may already be being used to monitor Americans' financial activity.

On June 23, 2022, the BSAAG Innovation and Technology Subcommittee held a meeting in which one item on the agenda was "AI/Machine Learning—new focus area."[208] Following this meeting, FinCEN and financial institutions exchanged ideas on how to incorporate and utilize AI to further track and report suspicious customer activity.[209] On September 19, 2023, a FinCEN

---

[205] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DIGITAL IDENTITY GUIDELINES: ENROLLMENT AND IDENTITY PROOFING (2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST DRAFTS REVISED GUIDELINES FOR DIGITAL IDENTIFICATION IN FEDERAL SYSTEMS (Dec. 16, 2022), https://www.nist.gov/news-events/news/2022/12/nist-drafts-revised-guidelines-digital-identification-federal-systems. *See also* Jay Stanley, *TSA Shouldn't Force a Bad Digital ID System on America*, ACLU (Oct. 31, 2023); Brett Solomon, *Digital IDs Are More Dangerous Than You Think*, WIRED (Sep. 28, 2018).

[206] *Brick & Mortar to Bits & Bytes: Adopting the U.S. AML/CFT Regime for Digital Identity*, BSAAG FinTech/RegTech Working Group (SCHWAB_HJC_00000737) (emphasis added).

[207] *Oversight of the Financial Crimes Enforcement Network: Hearing Before the H. Comm. on Fin. Serv.*, 117th Cong. (2022) (statement of Himamauli Das, Acting Director, Fin. Crimes Enf't Network).

[208] BSAAG Innovation and Technology Subcommittee Meeting (June 23, 2022, 2:00 PM) (JPM_HJC_0001917).

[209] *See* Email from personnel at Promontory Financial Group to BSAAG, FDIC employee, FinCEN liaison, and personnel at HSBC and Barclays (Aug. 18, 2022 1:58 PM) (118HJC_00005933).

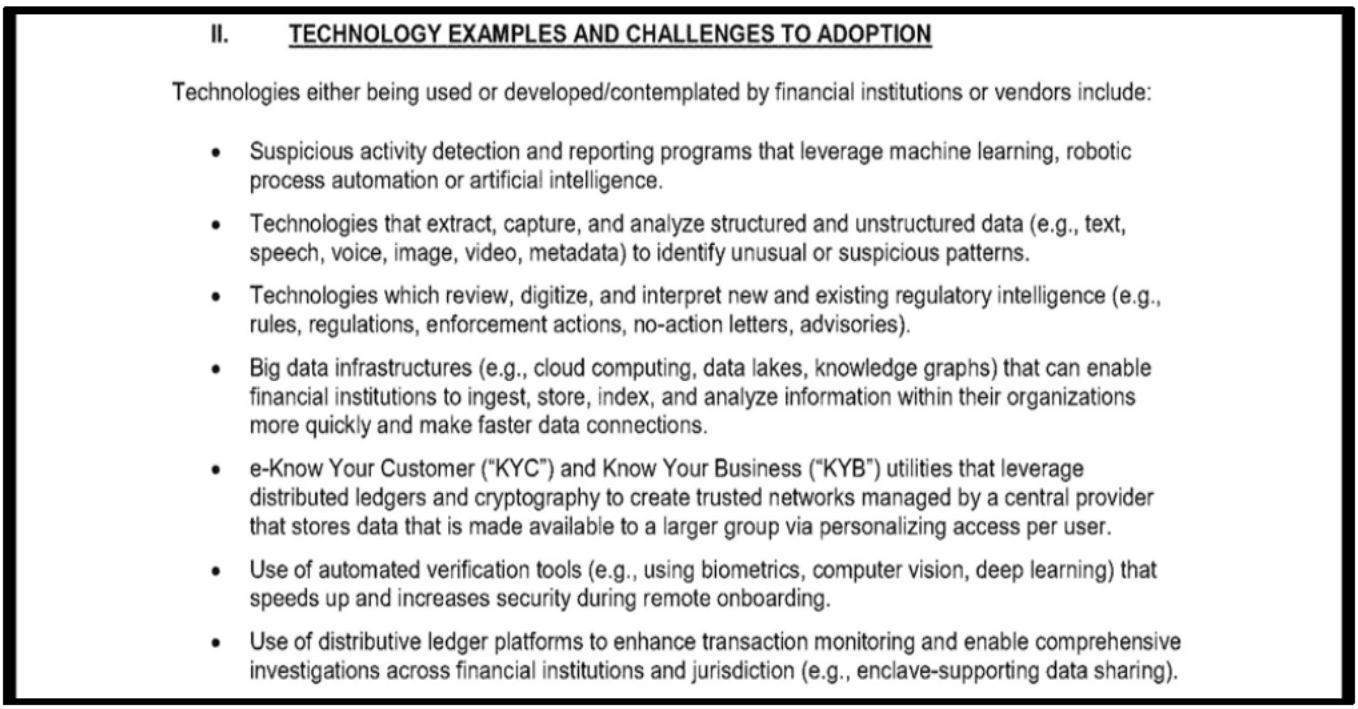
liaison sent an email to the AI and ML working group calling for volunteers to draft a white paper on its risks and benefits.[210]

As the Committee and Select Subcommittee have discussed in other reports, the growth and expansion of AI present major risks to Americans' civil liberties.[211] For example, the Committee and Select Subcommittee uncovered AI being used to censor "alleged misinformation regarding COVID-19 and the 2020 election . . . ."[212] Those concerns are not hypothetical. Some AI systems developed by Big Tech companies have been programmed with biases; for example, Google's Gemini AI program praised liberal views while refusing to do the same for conservative views, despite claiming to be "objective" and "neutral."[213] With financial institutions seemingly adopting AI solutions to monitor Americans' transactions, a similarly biased AI program could result in the systematic flagging or censoring of transactions that the AI is trained to view as "suspicious."[214] Given that financial institutions and federal law enforcement previously worked together to flag transactions using biased search terms like "TRUMP" or "MAGA," in addition to FinCEN sharing typologies that treated purchases of "religious texts" or "donations to organizations known to promote radicalism," as "indicators" of "homegrown violent extremism," concerns over biased AI transaction monitoring are well-founded.[215] If financial institutions are using a biased AI to spy on Americans' transactions, they may begin flagging purchases associated with conservative views such as lawful firearm purchases, tickets to conservative political rallies, or even Bibles—all constitutionally-protected activities.

The BSAAG appears to support using AI and other innovative technologies to monitor customers' transactions. Another document drafted by a BSAAG working group noted that "[e]ncouraging the adoption of innovative technologies is a priority for industry, law enforcement and regulators to increase the efficiency and effectiveness of AML/CFT programs . . . ."[216] The BSAAG document proposed, among other things, using "[s]uspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence" to monitor Americans' transactions surreptitiously, without human input.[217] The white paper also encouraged "[b]ig data infrastructures . . . that can enable financial institutions to ingest, store, index, and analyze information . . . ."[218]

---

[210] Email from FinCEN liaison, to BSAAG AI/ML Working Group members (Sept. 19, 2023, 2:24 PM) (SCHWAB_HJC_00001209).
[211] *See, e.g.*, STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE SPEECH "AT SCALE" AND TRYING TO COVER UP ITS ACTIONS (Comm. Print 2024).
[212] *Id.* at 1.
[213] Timothy Carney, *Gemini, Google's AI, tells very familiar lies*, THE WASHINGTON EXAMINER (Feb. 26, 2024).
[214] April Levin, *How AI is Revolutionizing Financial Crime Prevention in Banking*, SUPERIOR PRESS (June 4, 2024), https://www.superiorpress.com/blog/ai-financial-crime.
[215] STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).
[216] BSAAG Innovation and Adoption Working Group Recommendations (JPM_HJC_0002612).
[217] *Id.*
[218] *Id.*



II. TECHNOLOGY EXAMPLES AND CHALLENGES TO ADOPTION

Technologies either being used or developed/contemplated by financial institutions or vendors include:

- Suspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence.
- Technologies that extract, capture, and analyze structured and unstructured data (e.g., text, speech, voice, image, video, metadata) to identify unusual or suspicious patterns.
- Technologies which review, digitize, and interpret new and existing regulatory intelligence (e.g., rules, regulations, enforcement actions, no-action letters, advisories).
- Big data infrastructures (e.g., cloud computing, data lakes, knowledge graphs) that can enable financial institutions to ingest, store, index, and analyze information within their organizations more quickly and make faster data connections.
- e-Know Your Customer ("KYC") and Know Your Business ("KYB") utilities that leverage distributed ledgers and cryptography to create trusted networks managed by a central provider that stores data that is made available to a larger group via personalizing access per user.
- Use of automated verification tools (e.g., using biometrics, computer vision, deep learning) that speeds up and increases security during remote onboarding.
- Use of distributive ledger platforms to enhance transaction monitoring and enable comprehensive investigations across financial institutions and jurisdiction (e.g., enclave-supporting data sharing).

"Technologies either being used or developed/contemplated by financial institutions or vendors include: [s]uspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence."
—BSAAG Innovation and Adoption Working Group

In other words, the BSAAG document explored how financial institutions can make greater use of Americans' financial data and extract additional information on behalf of law enforcement and sought greater collaboration with "law enforcement, regulators, financial service providers, vendors, and technology companies" in order to "facilitat[e] the adoption of new technologies . . . ."[219]

Unfortunately, the BSAAG document glosses over any real concern for Americans' financial privacy and makes no mention of civil liberties, and, instead, prioritizes the interests of the financial industry, law enforcement, and new technologies designed to provide them with even greater insight into Americans' financial habits and their pattern of life. Documents uncovered in this investigation reveal that the financial information-sharing regime continues to grow alongside the financial institutions' capacity to surveil Americans.

POTENTIAL LEGISLATIVE REFORMS

Congress enacted the BSA and other relevant pieces of Anti-Money Laundering legislation with the stated goal of curbing money laundering, terrorist financing, and detecting and deterring other crimes.[220] However, the aims of that legislation has fallen short, while

[219] *Id.* at 0002613.
[220] *See* FED. DEPOSIT INSURANCE CORP., BANK SECRECY ACT / ANTI-MONEY LAUNDERING (BSA/AML).

needlessly sacrificing Americans' financial privacy. Based upon the Committee's and Select Subcommittee's findings, Congress should act to protect Americans' financial privacy.

The Financial Reporting Threshold Modernization Act proposes, among other things, raising the CTR threshold from the $10,000 mark—set more than 50 years ago—to $60,000.[221] The original $10,000 CTR threshold, was set "to identify unusually large currency transactions that exceed the legitimate and customary conduct of a bank's customers, and produce information highly useful to combat financial crime[;]" however, if the CTR threshold were adjusted for inflation, it would be nearly $75,000 today.[222] For that reason, the $10,000 threshold actually makes the program less effective as the sheer number of CTR reports—20.8 million in 2023—transforms the CTR from being about criminal activity into a government surveillance program. If inflation trends continue, the number of transactions passing the $10,000 threshold will continue to increase, resulting in even more CTR filings and greater surveillance of Americans' finances.

Congress could also consider reforming the SAR filing process. Under the current BSA framework, financial institutions are required to act as confidential informants on their customers, reporting them to the federal government without any recourse or notice available to the customer. Congress could amend the BSA to require that banks, after a certain period of time, give notice to the customer that a SAR was filed, provide a justification, and offer an opportunity for the customer to respond to allegations they engaged in "suspicious activity." Other reforms propose establishing "a private right of action for Americans and financial institutions harmed by illicit government activity."[223]

Finally, Congress could restore Fourth Amendment protections to Americans' financial records. In order to end warrantless surveillance, Congress could require a warrant before law enforcement can gain access to Americans' private financial information. Senator Mike Lee's Saving Privacy Act proposes bolstering the warrant requirement under the Right to Financial Privacy Act of 1978.[224] Americans should not have to choose between having a bank account and worrying that the federal government may have warrantless access to their personal financial decisions and other revealing details about their pattern of life, interests, faith, politics, and more.

---

[221] Financial Reporting Threshold Modernization Act, H.R.8686, 118th Cong. (2024).
[222] American Bankers Association, *Letter to FinCEN on Information Collection Requirements relating to Currency Transaction Reports* (Apr. 5, 2024); *see also* Nicholas Anthony, *How Inflation Erodes Financial Privacy*, CATO (June 10, 2022).
[223] *See* Press Release, Sen. Mike Lee, Lee Introduces the Saving Privacy Act to Protect Americans' Financial Data (Sept. 25, 2024); *see also* Saving Privacy Act, S. 5242, 118th Cong. (2024).
[224] S. 5242 (2024).

CONCLUSION

The Committee and Select Subcommittee opened this investigation to determine how and to what extent the federal government and financial institutions weaponized financial surveillance to monitor the private lives of American citizens. The result of the investigation reveals that financial surveillance goes far beyond the targeting of one political ideology and is more pervasive than one act of criminal conduct. The information-sharing apparatus, designed by Congress and implemented by the Executive Branch and financial institutions, has been warped into a tool designed to constantly monitor the activities of millions of Americans.

Federal law enforcement has shown that it will leverage any opportunity to operate outside the bounds of the statutes that govern access to Americans' financial data. Because the existence of a SAR and other BSA filings may never be revealed to a customer, Americans may never know the extent to which their finances are being tracked. The most egregious abuses of this system occurred in the days after January 6, 2021, in which seemingly anyone with any possible connection to Washington, D.C., was potentially subjected to warrantless government surveillance and SAR filings. It is very likely that, without intervention or reform, federal law enforcement will abuse this system again in the future.

Indeed, the information gathered by the Committee and Select Subcommittee shows that the federal government continues to exploit the laws governing financial data and is deputizing financial institutions as arms of law enforcement. By sharing typologies and even specific names with financial institutions, federal law enforcement has shown its willingness to manipulate the SAR filing process. Although the FBI and FinCEN claim that financial institutions have the choice to act upon the information federal law enforcement shares, the reality is different. When federal law enforcement demands something, it is difficult—if not impossible—for banks to say no.

As the federal government and financial institutions adjust to modern finance, there will come a time when almost no financial activity will occur outside of the watchful eye of the federal government. And as the federal government and the financial sector explore integrating new technologies like digital ID and the use of AI to monitor transactions, every financial movement of every American could soon be automatically recorded and scrutinized. With the documented abuses of AI technology already mounting, these new tools pose a threat of biased enforcement.

Absent adequate congressional oversight and legislative reforms, it is likely that countless more Americans will be subject to financial surveillance and potentially federal investigation, all without ever knowing about it. The Committee and Select Subcommittee will continue to investigate the coordination between Big Banks and Big Government to protect Americans' civil liberties.