



**FINANCIAL SURVEILLANCE IN THE UNITED STATES:
HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL
INSTITUTIONS 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



March 6, 2024

EXECUTIVE SUMMARY

The Committee on the Judiciary and its Select Subcommittee on the Weaponization of the Federal Government are charged by the House of Representatives with upholding fundamental American civil liberties.¹ As a part of this mission, the Committee and Select Subcommittee have uncovered startling evidence that the federal government was engaged in broad financial surveillance, prying into the private transactions of American consumers. This financial surveillance was not predicated on any specific evidence of particularized criminal conduct and, even worse, it keyed on terms and specific transactions that concerned core political and religious expression protected by the Constitution.

On February 7, 2023, the Committee and Select Subcommittee received testimony from retired Federal Bureau of Investigation (FBI) Supervisory Intelligence Analyst George Hill.² During his transcribed interview, Mr. Hill testified that, following the events at the U.S. Capitol on January 6, 2021, Bank of America (BoA), voluntarily and without legal process, provided the FBI with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region between the dates of January 5 and January 7, 2021.³ Mr. Hill also testified that this BoA “data dump” of customer information also included a list of individuals who had *ever* used a BoA credit or debit card to purchase a firearm, regardless of when or where it was purchased.⁴ This testimony was later confirmed by another former senior FBI official, Joseph Bonavolonta.⁵ In fact, when the BoA information was brought to the attention of Steven Jensen, the then-Section Chief of the FBI’s Domestic Terrorism Operations Section, he acted to “pull” the BoA information from FBI systems because the “leads lacked allegations of federal criminal conduct,” and out of “concern[.]” from where it “originated.”⁶

In response to this testimony, 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.⁷ In the months that followed this initial request, the Committee and Select Subcommittee’s oversight has uncovered the magnitude of law enforcement’s access to private financial records of American citizens.

These documents show that following the events of January 6, 2021, federal law enforcement officials from the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) and the FBI initiated multiple discussions with financial institutions.⁸ These meetings included some of the largest financial institutions in the United States, including Barclays, U.S. Bank, Charles Schwab, HSBC, BoA, Paypal, KeyBank, Standard Chartered, Western Union,

¹ Rules of the U.S. House of Representatives, R. X (2023); H. Res. 12, 118th Cong. (2023).

² Transcribed Interview of Mr. George Hill (Feb. 7, 2023).

³ *Id.* at 74-76.

⁴ *Id.*

⁵ Transcribed Interview of Mr. Joseph Bonavolonta at 13 (May 4, 2023).

⁶ Transcribed Interview of Mr. Steven Jensen at 149, 150, 152 (May 19, 2023).

⁷ *See, e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp. (May 25, 2023).

⁸ *See, e.g.*, BofA-HJUD-00000008, 11, 14, 15, 16, 22, 29, 33.

Wells Fargo, Citibank, Santander, JPMorgan Chase, and MUFG.⁹ These meetings were geared toward discussing options for financial institutions to share customer information voluntarily with federal law enforcement outside of normal legal processes.¹⁰

The information obtained by the Committee and Select Subcommittee also shows that law enforcement and private institutions shared intelligence products in the aftermath of January 6 through a web portal run by the Domestic Security Alliance Council (DSAC).¹¹ The DSAC is a public-private partnership led by the FBI's Office of Private Sector and the Department of Homeland Security's (DHS) Office of Intelligence and Analysis.¹² The DSAC promotes the "exchange of security and intelligence information" between the federal government and its 650 "member" companies, collectively comprising "two-thirds of the U.S. Gross Domestic Product" and "35 million employees."¹³ Following January 6, the FBI shared an intelligence product titled "Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach," prepared by the FBI, DHS, and the National Counterterrorism Center (NCTC), with financial institutions to alert them to individuals that may fit the profile of criminal and domestic violent extremists (DVEs).¹⁴

This FBI intelligence product, along with other materials shared by federal law enforcement, detail the extent to which federal law enforcement derisively viewed American citizens. For example, one report shared with financial institutions noted that those Americans who expressed opposition to firearm regulations, open borders, COVID-19 lockdowns, vaccine mandates, and the "deep state" may be potential domestic terrorists.¹⁵ Federal law enforcement used this report and materials like it to commandeer financial institutions' databases and ask the financial institutions to conduct sweeping searches of individuals not suspected of committing any crimes. For example, federal law enforcement suggested that banks filter Zelle payments using keywords like "MAGA" and "TRUMP" as part of an ostensible investigation into the events on January 6, 2021, and also warned that "the purchase of books (including religious texts) and subscriptions to other media containing extremist views," could be evidence of "Homegrown Violent Extremism."¹⁶

FinCEN also distributed materials to financial institutions instructing them on how to use Merchant Category Codes (MCCs) to search through transactions to detect potential criminals or "extremists."¹⁷ These MCCs use keywords to comb through transactions, such as "small arms" purchases or recreational stores such as "Cabela's," "Bass Pro Shop," and "Dick's Sporting Goods."¹⁸ Americans doing nothing other than shopping or exercising their Second Amendment rights were being tracked by financial institutions and federal law enforcement. Despite these

⁹ *Id.*; See also USBANK_HJC_000032.

¹⁰ See, e.g., USBANK_HJC_000032.

¹¹ See, e.g., BofA-HJUD-00000051.

¹² See *About DSAC*, DOMESTIC SECURITY ALLIANCE COUNCIL, <https://www.dsac.gov/about> (last visited Jan. 17, 2024).

¹³ *Id.*

¹⁴ See, e.g., BofA-HJUD-00000040.

¹⁵ BofA-HJUD-00000041, 42.

¹⁶ HJC118_00000006, 7.

¹⁷ See, e.g., HJCSWFG_0000454.PPTX.

¹⁸ *Id.* at 4.

transactions having no criminal nexus, FinCEN seems to have adopted a characterization of these Americans as potential threat actors and subject to surveillance.

Without the FBI whistleblowers' disclosures to the Committee and Select Subcommittee, these documents would not have come to light. While it is alarming enough that federal law enforcement and Bank of America used January 6, 2021, as a pretext for surveilling potentially thousands of Americans without a warrant, the documents received by the Committee and Select Subcommittee show a pattern of financial surveillance aimed at millions of Americans who hold conservative viewpoints or simply exercise their Second Amendment rights. This raises serious concerns and doubts about federal law enforcement's and financial institutions' commitment to respecting Americans' privacy rights and fundamental civil liberties.

As the investigation continues, the Committee and Select Subcommittee will continue to work to understand the extent and status of this widespread financial surveillance while also exploring how Congress could enact legislation to further protect Americans' civil liberties.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

TABLE OF CONTENTS 4

BACKGROUND..... 5

THE STATUTORY FRAMEWORK FOR ACCESS TO AMERICANS’ PRIVATE FINANCIAL DATA..... 8

 A. The Right to Financial Privacy Act..... 8

 B. Section 314(a) of the USA Patriot Act..... 9

 C. The Bank Secrecy Act..... 10

FINANCIAL SURVEILLANCE OF AMERICAN CONSUMERS..... 13

 A. Federal law enforcement used informal meetings and backchannel discussions with financial institutions to devise the best methods for gathering Americans’ private financial information..... 13

 B. Federal law enforcement circulated politicized materials that evidenced hostility towards conservative viewpoints and weaponized financial institutions’ databases by treating lawful transactions as suspicious..... 14

 i. Federal law enforcement shared information equating conservative beliefs with domestic terrorism through a controlled-access portal managed by the “Domestic Security Alliance Council.” 14

 ii. The FBI commandeered financial institutions’ databases to conduct sweeping searches without an individualized nexus to particularized criminal conduct..... 18

CONCLUSION..... 35

BACKGROUND

As part of the oversight conducted by the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government, the Committee and Select Subcommittee received testimony from retired FBI Supervisory Intelligence Analyst George Hill on February 7, 2023.¹⁹ Mr. Hill testified that Bank of America (BoA) provided the FBI—voluntarily and without any legal process—with a list of individuals who had made transactions in the Washington, D.C., metropolitan area with a BoA credit or debit card between January 5 and January 7, 2021, and that individuals who had previously purchased a firearm with a BoA debit card or credit card were elevated to the top of the list regardless of when or where the purchase was made.²⁰

In his transcribed interview, Mr. Hill stated:

The Bank of America, with no directive from the FBI, data-mined its customer base. And they data-mined a date range of 5 to 7 January [of 2021] any BOA customer who used a BOA product. And by ‘BOA product,’ I mean a debit card or a credit card. They compiled that list. And then, on top of that list, they put anyone who had purchased a firearm during any date. So it was a huge list²¹

Mr. Hill’s testimony was corroborated by the testimony of his former supervisor and former Special Agent-in-Charge of the Boston Field Office, Joseph Bonavolonta.²² Mr. Bonavolonta testified that Boston’s Joint Terrorism Task Force Squad Supervisor, Chief Division Counsel, and Assistant Special Agent-in Charge of Counterterrorism also brought the BoA data to his attention.²³ Mr. Bonavolonta testified:

[A] lead had been sent to our office from a unit within FBI Headquarters that fell under the Office of Private Sector . . . in the body of the lead, there was . . . information that was provided by Bank of America following a certain number of criteria that in essence aggregated a list of individuals that were supposedly living up in the New England area who . . . either had potentially made . . . certain credit card purchases . . . for hotel reservations or plane tickets, or potential purchases at certain gun stores in and around . . . January 6th or planned for the inauguration date.²⁴

Mr. Bonavolonta also testified that, “one of the [list’s] criteria . . . in terms of Bank of America’s data . . . was related to purchases that had been made at either gun shops or, you

¹⁹ See Transcribed Interview of Mr. George Hill (Feb. 7, 2023).

²⁰ *Id.* at 74-76.

²¹ *Id.* at 74.

²² See Transcribed Interview of Mr. Joseph Bonavolonta at 12 (May 4, 2023).

²³ *Id.* at 11.

²⁴ *Id.* at 12.

know, stores that would sell firearms.”²⁵ Mr. Bonavolonta also stated that the BoA customer data was sent to other FBI field offices across the country, including the Springfield, Illinois field office.²⁶

Mr. Bonavolonta’s testimony was further supported by Steven Jensen, the then-Section Chief of the FBI’s Domestic Terrorism Operations Section. In his transcribed interview, Mr. Jensen testified that the FBI “maintain[s] partnerships with the private sector, to include Bank of America” and that he was “aware that they provided information to the FBI,” but that, to his knowledge, the FBI did not ask for this information from BoA.²⁷ Instead, he testified that the information “was certain purchaser transaction records of individuals that Bank of America provided over to the FBI that wasn’t requested by the FBI. It was of their own volition . . . without any process being issued.”²⁸ When that information was brought to his attention, Mr. Jensen acted to “pull” the BoA information from FBI systems because “the leads lacked allegations of federal criminal conduct,” and out of “concern[]” from where “it originated.”²⁹ At a hearing before the Committee on July 12, 2023, FBI Director Chris Wray responded to a question about the BoA information and stated that “a number of business community partners all the time, including financial institutions, share information with us about possible criminal activity In the specific instance that you’re asking about, my understanding is that that information was shared with field offices for information only, but, then, recalled to avoid even the appearance of any kind of overreach.”³⁰

Mr. Hill, Mr. Bonavolonta, and Mr. Jensen’s testimony raise serious concerns about federal law enforcement’s compliance with existing legal processes designed to protect Americans’ financial privacy. In light of these revelations, the Committee and the Select Subcommittee requested information from BoA and six other financial institutions to understand how and to what extent financial institutions worked with federal law enforcement to collect, share, and monitor Americans’ data.³¹ In response to these requests, the Committee and Select Subcommittee have received, to date, over a thousand pages of documents from six of the largest financial institutions in the United States, that, together, are responsible for managing trillions of dollars in assets and millions of Americans’ bank accounts.³² Although the former FBI officials

²⁵ *Id.* at 17.

²⁶ *Id.* at 13.

²⁷ Transcribed Interview of Mr. Steven Jensen at 146-47 (May 19, 2023).

²⁸ *Id.* at 147, 150.

²⁹ *Id.* at 149-50, 152.

³⁰ See *Oversight of the Federal Bureau of Investigation Before the H. Comm. on the Judiciary*, 118th Cong. (2023).

³¹ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp (May 25, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. William S. Demchak, Chief Exec. Officer of PNC Fin. Serv. (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Andrew Cecere, Chief Exec. Officer of U.S. Bancorp (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Charles W. Scharf, Chief Exec. Officer of Wells Fargo (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. William H. Rogers, Chief Exec. Officer of Truist Fin. Corp. (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Jane Fraser, Chief Exec. Officer of Citigroup (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. James Dimon, Chief Exec. Officer of JPMorgan Chase & Co. (June 12, 2023).

³² See FEDERAL RESERVE STATISTICAL RELEASE: LARGE COMMERCIAL BANKS (2023); see also Steve Cocheo, *JPMorgan Chase Defends Contrarian Branch Strategy as Deposit-Gathering Machine*, THE FIN. BRAND (May 24, 2023).

who testified before the Committee and Select Subcommittee believed that BoA acted alone in sending customer data to federal law enforcement, the documents indicate that federal law enforcement encouraged financial institutions to engage in financial surveillance of American citizens. These documents shed light on back-channel networks that facilitate discussions between financial institutions and federal law enforcement, as well as the information-sharing methods that federal law enforcement used as part of an ostensible investigation into the events of January 6.

The emergence of credit cards, mobile banking, and other digital marketplaces have resulted in an unprecedented amount of private data entrusted to financial institutions, potentially revealing all sorts of sensitive information about a customer.³³ For that reason, financial records have become an important investigative tool for federal law enforcement.³⁴ Still, federal law enforcement's interest in financial records must be weighed against the privacy interests of Americans. Without greater oversight and the necessary legislative reforms reflecting the advances in modern-day banking practices, Americans' private financial data is still vulnerable to the shortcomings of an outdated legal framework and pervasive government surveillance.

In 1976, the Supreme Court of the United States held in *United States v. Miller* that customers of financial institutions have no reasonable expectation of privacy in documents voluntarily conveyed to a third party.³⁵ In effect, that decision meant that law enforcement did not have to obtain a warrant in order to retrieve bank records held by a financial institution.³⁶ The *Miller* decision triggered Congress to enact the Right to Financial Privacy Act of 1978 (RFPA), which afforded some privacy protections to financial records held by a third party.³⁷ Most notably, the RFPA requires law enforcement to utilize certain legal processes as a condition of receiving financial records, subject to a number of exceptions.³⁸ In addition, the Bank Secrecy Act (BSA) imposes additional reporting obligations on financial institutions and Section 314(a) of the USA Patriot Act of 2001 gave federal law enforcement greater access to account information entrusted to financial institutions.³⁹ From the information obtained by the Committee and Select Subcommittee, these pieces of legislation have failed to adequately protect Americans' financial information. What it has left is an expansive, backdoor information-sharing regime led by the nation's most powerful law enforcement agencies and their partners in the financial sector.

A. The Right to Financial Privacy Act

In general, the RFPA protects customer information by limiting access to the "financial records of any customer from a financial institution unless the financial records are reasonably described" and the "government authority" receives customer consent, or the records are disclosed in accordance with certain notice requirements pursuant to an administrative subpoena, search warrant, judicial subpoena, or formal written request.⁴⁰ However, if one of the eighteen exceptions under the RFPA apply, legal process and notice may not be required.⁴¹ In some circumstances, these exceptions allow the FBI and the Financial Crimes Enforcement Network

³³ See Nicholas Anthony, *The Right to Financial Privacy*, CATO (May 2, 2023), <https://www.cato.org/policy-analysis/right-financial-privacy>.

³⁴ See, e.g., FINANCIAL CRIMES ENFORCEMENT NETWORK, LAW ENFORCEMENT OVERVIEW.

³⁵ 425 U.S. 435, 442-46 (1976).

³⁶ See *id.* at 446.

³⁷ See Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423; see also Nicholas Anthony, *supra* note 33.

³⁸ See, e.g., 12 U.S.C. § 3413.

³⁹ See FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN'S 314(A) FACT SHEET; see also FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.

⁴⁰ See 12 U.S.C. § 3402; see also 12 U.S.C. §§ 3404-3408.

⁴¹ See, e.g., 12 U.S.C. § 3413(g) (relating to disclosure pursuant to legitimate law enforcement inquiry).

(FinCEN), along with other government authorities, to pursue certain customer bank records without utilizing any legal process.⁴² Doing so, however, may limit the kinds of records the requester may receive.⁴³

Under many circumstances, the exceptions to the RFPA function as the rule. For example, the RFPA does not permit the “withholding of financial records or information required to be reported in accordance” with any other statute or rule⁴⁴ and allows financial institutions to voluntarily notify any “[g]overnment authority that such institution, or officer, employee, or agent has information which *may be relevant to a possible violation of any statute or regulation.*”⁴⁵ The customer has no redress available against the institution for such a disclosure or for its failure to provide the customer with notice.⁴⁶ Another exception to the RFPA allows for “disclosure pursuant to legitimate law enforcement inquiry.”⁴⁷ That exception permits law enforcement to seek the “name, address, account number, and type of account of any customer or ascertainable group of customers associated with a financial transaction or class of financial transactions”⁴⁸ Similarly, the RFPA does not protect . . . against actions initiated by the U.S. Secret Service or other “government authorit[ies] authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities . . . or a government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.”⁴⁹ The FBI is also excepted from the RFPA’s general protections and legal process requirements if the FBI certifies to a financial institution that the records are “sought for foreign intelligence purposes to protect against international terrorism or clandestine intelligence activities.”⁵⁰ The financial institution is generally prohibited from disclosing to any person, including its impacted customers, that any such intelligence-related request has been made.⁵¹

B. Section 314(a) of the USA Patriot Act

Section 314(a) of the USA PATRIOT Act of 2001 required the Secretary of the Treasury to “adopt regulations to encourage regulatory and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.”⁵² The law authorized “federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be

⁴² *Id.*

⁴³ *Id.*

⁴⁴ 12 U.S.C. § 3413(d).

⁴⁵ 12 U.S.C. § 3403(c) (emphasis added).

⁴⁶ *Id.*

⁴⁷ 12 U.S.C. § 3413(g).

⁴⁸ *Id.*

⁴⁹ 12 U.S.C. § 3414(a)(1).

⁵⁰ 12 U.S.C. § 3414(a)(5).

⁵¹ 12 U.S.C. § 3414(c).

⁵² FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN’S 314(A) FACT SHEET (Feb. 26, 2019), [https://www.fincen.gov/sites/default/files/shared/314\(a\)%20FACTS%20AND%20FIGURES.pdf](https://www.fincen.gov/sites/default/files/shared/314(a)%20FACTS%20AND%20FIGURES.pdf).

involved in terrorism or money laundering.”⁵³ When a request is received, “financial institutions must query their records for data matches,” and then report whether there is a positive match to FinCEN within two weeks of receiving the request.⁵⁴ These requests are subject to strict confidentiality requirements prohibiting their disclosure.⁵⁵

Put differently, federal law enforcement is able to direct more than 16,000 financial institutions to conduct a search of their financial records if law enforcement “reasonably suspect[s], based on credible evidence,” that the suspected individual or entity is engaging in terrorist activity or money laundering.⁵⁶ If the financial institution identifies a positive match, it reports to FinCEN the name, account and transaction, as well as the social security number, taxpayer identification, passport number or any other identifying information related to the individual.⁵⁷ This is done without any judicial involvement.⁵⁸ The Committee and Select Subcommittee have obtained documents indicating that federal law enforcement invoked its “terrorist activity” authority under Section 314(a) as a part of its investigation into the events at the U.S. Capitol on January 6, 2021.⁵⁹

C. The Bank Secrecy Act

Finally, the Bank Secrecy Act (BSA) authorizes the Department of the Treasury to impose certain far-reaching reporting obligations on businesses and financial institutions.⁶⁰ As part of these requirements, financial institutions must file a Currency Transaction Report (CTR) with FinCEN reflecting the information of any individual involved in any transaction of over \$10,000, including the individual’s government-issued identification and Social Security Number.⁶¹ The BSA also “requires that a bank or other financial institution file a SAR [suspicious activity report] whenever it identifies a ‘suspicious transaction *relevant to a possible violation of law or regulation*,’”⁶² while placing a *de facto* gag order on financial institutions prohibiting the revelation of “any information that would reveal the transaction has been reported” to any third party.⁶³ Indeed, “SARs contain personally identifiable information about

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ 31 C.F.R. § 1010.520(b)(3)(iv)(B).

⁵⁶ 31 C.F.R. § 1010.520(b)(3).

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ TFC000007-8; *see also* Letter from John Adams, Legal Counsel for Truist. Fin. Corp., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary (July 18, 2023) (discussing “several channels through which banks routinely communicate with law enforcement,” that include “responding to requests for account information governed by Section 314(a) of the Patriot Act.”).

⁶⁰ *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.

⁶¹ *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE; *see also Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI) Before the H. Comm. on Financial Services*, 118th Cong. 2 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.) (observing that the value of \$10,000 in 1974 at the time of the BSA’s enactment is roughly worth \$63,900 today).

⁶² 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).

⁶³ *See* 31 U.S.C. 5318(g)(1); *see also* 31 C.F.R. § 1020.320; Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary (June 22, 2023) (discussing the Bank Secrecy Act and obligations to “confidentially report potentially suspicious activity”).

individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation . . . subject to strong confidentiality protections”⁶⁴ The BSA also grants broad immunity to “[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency.”⁶⁵ By contrast, failure to file a SAR can result in large monetary penalties.⁶⁶ This creates a strong incentive for financial institutions to file defensively, even when there is little reason to do so.⁶⁷

In other words, the BSA shields financial institutions from ever facing liability for any disclosure made to law enforcement regarding its customers’ transactions—regardless of the financial institutions’ reasonableness or motivations—and the institution never has to disclose to the customer that the transaction was reported to law enforcement, leaving meaningful judicial review lacking. The BSA also cloaks the reporting of a “suspicious transaction” activity report in a nearly impenetrable veil, which some banks have used in an attempt to shield these reports from congressional oversight.⁶⁸ Combined, this framework treats banks as agents of the government and obstructs congressional oversight of federal law enforcement and its relationship with the financial sector, leaving the American financial system ripe for pervasive surveillance. Indeed, the Supreme Court of the United States has expressed skepticism about the BSA’s reporting requirements in considering its constitutionality, noting in a 1974 opinion that the “reporting requirements . . . would pose substantial and difficult constitutional questions” and warning that “the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process.”⁶⁹

To illustrate the breadth of the BSA’s reporting requirements, FinCEN announced that in 2019 it received over 20 million filings from more than 97,000 financial institutions as required by the BSA.⁷⁰ According to FinCEN, those filings “provid[ed] a *wealth of potentially useful* information to [government] agencies”⁷¹ Among those BSA-required filings, FinCEN reported that it received over 4.3 million SARs in 2022, nearly doubling from the number it received in 2019. FinCEN also reported that “Other Suspicious Activities” was the most reported reason for filing a SAR, with “terrorist financing” as one of the least reported SAR activity

⁶⁴ Letter from Corey Tellez, *supra* note 62 at 2.

⁶⁵ 31 U.S.C. 5318(g)(3).

⁶⁶ 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”).

⁶⁷ *Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI) 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.).

⁶⁸ *See, e.g.*, Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2-3 (June 22, 2023) (discussing confidentiality under the Anti-Money Laundering Act and Bank Secrecy Act.).

⁶⁹ 416 U.S. 21, 79-80 (1974).

⁷⁰ Nicholas Anthony, *Reporting FinCEN’s Suspicious Activity*, CATO (Apr. 13, 2022), <https://www.cato.org/blog/reporting-fincens-suspicious-activity>.

⁷¹ *Id.* (emphasis added).

types.⁷² This means that FinCEN is using the BSA and its SAR reporting requirements to track far more transactions than just those limited to money laundering and terrorist financing. Similarly, FinCEN reported that it received over 20.6 million CTRs in 2022, averaging to nearly 56,500 per day.⁷³ A CTR contains sensitive financial data and is required to be filed for any transaction over \$10,000, regardless of whether anything about that transaction is “suspicious” or otherwise related to criminal activity.⁷⁴

As a result, a vast amount of personal financial information is regularly shared with FinCEN and, in turn, to other law enforcement agencies via a searchable BSA database.⁷⁵ For example, in 2020, “FinCEN reported that DOJ agencies conducted more than 500,000 searches of SARs through its database.”⁷⁶ However, neither Congress nor American consumers have any real access to examine the propriety of the SARs or law enforcement’s use of them.⁷⁷ The Committee and Select Subcommittee’s investigation has obtained documents revealing that SARs were likely filed on sprawling classes of transactions and individuals despite the lack of any link to criminal—or even “suspicious”—activity.

⁷² FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) YEAR IN REVIEW FOR FY 2022 (2023); *see also Special Report: suspicious activity reports surge; 2023 filings on pace for another record*, THOMSON REUTERS (June 9, 2023).

⁷³ FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) YEAR IN REVIEW FOR FY 2022 (2023).

⁷⁴ *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE.

⁷⁵ U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-22-105-242, BANK SECRECY ACT: ACTION NEEDED TO IMPROVE DOJ STATISTICS ON USE OF REPORTS ON SUSPICIOUS FINANCIAL TRANSACTIONS at 12 (2022).

⁷⁶ *Id.*

⁷⁷ *See, e.g.*, 31 U.S.C. 5318(g)(2)(A); 31 C.F.R. § 1020.320(e)(1).

The Committee and Select Subcommittee have obtained documents showing that federal law enforcement’s investigation, predicated on the events that transpired at the U.S. Capitol on January 6, 2021, devolved into a fishing expedition for Americans’ financial data. Federal law enforcement agencies, including FinCEN and the FBI, treated lawful transactions as suspicious and shared information with financial institutions through backdoor channels, often circulating materials exhibiting a clear animus towards conservative viewpoints. In addition, FinCEN and the FBI relied on Zoom discussions, private and online government-run portals, as well as sweeping searches of financial institutions’ records to conduct its investigation. Given the important civil liberties at stake, federal law enforcement’s overreach and political bias is alarming.

A. Federal law enforcement used informal meetings and backchannel discussions with financial institutions to devise the best methods for gathering Americans’ private financial information.

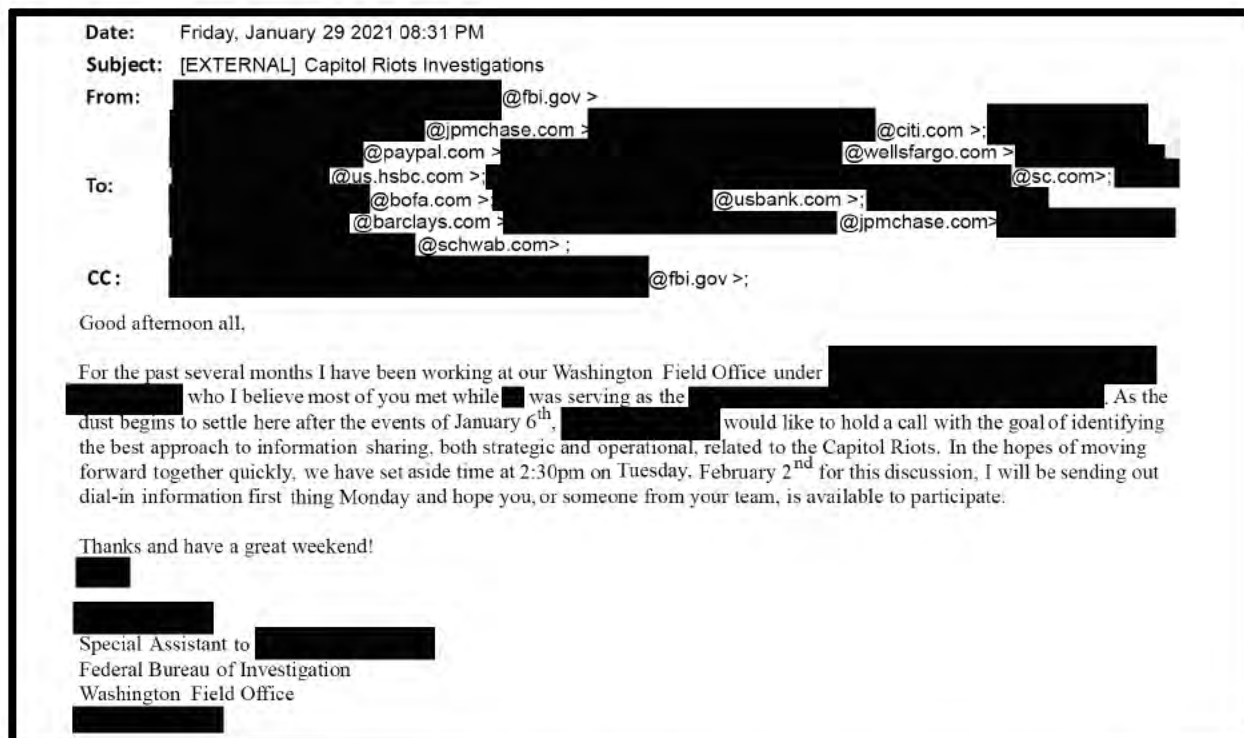
Federal law enforcement officials organized Zoom discussions with financial institutions as part of their investigation into the events of January 6, 2021.⁷⁸ Participants in these meetings included Barclays, U.S. Bank, Charles Schwab, HSBC, BoA, Paypal, KeyBank, Standard Chartered, Western Union, Wells Fargo, Citibank, Santander, JPMorgan Chase, Union Bank, and MUFG.⁷⁹ In one meeting, an FBI official from the Washington Field Office reached out to a number of financial institutions to arrange a meeting with the goal of “identifying the best approach to information sharing, both strategic and operational,” in the wake of the events of January 6.⁸⁰ At least five other Zoom meetings were scheduled by FinCEN officials and financial institutions and included the subject “Capitol Riots.”⁸¹ Viewed together, these meetings suggest that federal law enforcement officials were brainstorming informal methods—outside of normal legal processes—for obtaining private customer information from financial institutions.

⁷⁸ See, e.g., BofA-HJUD-00000008, 11, 14, 15, 16, 22, 29, 33; USBANK_HJC_000032 [hereinafter “Zoom Meetings”].

⁷⁹ *Id.*

⁸⁰ USBANK_HJC_000032.

⁸¹ Zoom Meetings, *supra* note 78.



B. Federal law enforcement circulated politicized materials that evidenced hostility towards conservative viewpoints and weaponized financial institutions’ databases by treating lawful transactions as suspicious.

Federal law enforcement circulated materials to financial institutions as part of an information-sharing operation that alerted financial institutions to the risk of customers and accounts that may be associated with conservative views.⁸² In particular, federal law enforcement attempted to cast swaths of lawful and otherwise harmless transactions as potentially suspicious.⁸³ Given that these materials were distributed to some of the largest financial institutions and companies in the world, their reach could potentially impact the transactions and accounts of hundreds of millions of customers without the customers ever knowing it.

i. Federal law enforcement shared information equating conservative beliefs with domestic terrorism through a controlled-access portal managed by the “Domestic Security Alliance Council.”

One way that information is shared from federal law enforcement to certain corporations and financial institutions is through an obscure government-run portal led by the Domestic Security Alliance Council (DSAC) that is only accessible to its “members.”⁸⁴

⁸² See, e.g., HJCSWFG_0000454.PPTX.

⁸³ See, e.g., BofA-HJUD-00000225.

⁸⁴ About DSAC, DOMESTIC SECURITY ALLIANCE COUNCIL, <https://www.dsac.gov/about> (last visited Jan. 17, 2024); see also BofA-HJUD-00000051.



The DSAC is a program spearheaded by the FBI’s Office of Private Sector Engagement Programs and Initiatives (OPS) and the Department of Homeland Security’s Office of Intelligence and Analysis that promotes “timely and effective exchange of security and intelligence information between the federal government and the private sector.”⁸⁵ According to the official website, the DSAC is a “corporate membership program,” that requires all of its members to be “for-profit” and “generate a minimum of \$1 billion in annual revenue”⁸⁶ Its mission includes facilitating “enduring relationships among its private sector member companies, across the FBI enterprise, and with the Department of Homeland Security (DHS) Headquarters . . . to detect, prevent, and deter criminal acts.”⁸⁷ Since its creation in 2005, “[t]he DSAC program has grown to include more than 650 member companies . . . collectively account[ing] for nearly two-thirds of the U.S. Gross Domestic Product and employ[ing] more than 35 million people.”⁸⁸ Through the DSAC portal, among other avenues, the FBI, DHS, and other government agencies are able to share non-public intelligence products, including Liaison Information Reports, with members of the private sector.⁸⁹

One such intelligence product, titled “Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach,” was shared as a Liaison Information Report and prepared by the FBI, DHS, and the National Counterterrorism Center (NCTC).⁹⁰ The FBI’s Office of Private Sector shared the report with financial institutions and other DSAC members on January 18,

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ FEDERAL BUREAU OF INVESTIGATION, OFFICE OF PRIVATE SECTOR, PRIVATE SECTOR ENGAGEMENT PROGRAMS AND INITIATIVES.

⁹⁰ BofA-HJUD-00000040.

2021 to “alert private sector partners that the 6 January 2021 violent breach by suspected domestic violent extremists (DVEs) into the U.S. Capitol Building may serve as a driver for a diverse set of DVEs.”⁹¹ In the report, the FBI described reasons that “may play in mobilizing criminal actors and DVEs to violence.”⁹² Among the reasons that may mobilize DVEs to violence is “the belief in the existence of global or ‘deep state’ actors who work to manipulate various social, political and/or economic conditions”⁹³ It also assesses that “DVEs’ efforts to engage in violence at lawful gatherings will probably increase throughout 2021, as some DVEs perceive increased socio-political pressures.”⁹⁴ Those “pressures” mobilizing DVEs to violence, in the eyes of the FBI, included opposition to “firearm legislation, the easing of immigration restrictions, and new limits on the use of public land,” as well as “narratives by DVEs that the 2020 General Election was illegitimate,” or “discontent with renewed measures to mitigate the spread of COVID-19, the ordered dissemination of COVID-19 vaccinations, and the efficacy and/or safety of COVID-19 vaccinations.”⁹⁵

TOP SECRET

OFFICE OF PRIVATE SECTOR LIAISON INFORMATION REPORT (LIR)

Range of DVE Actors Likely to Pose Increasing Threat at Lawful Protests, Rallies, Demonstrations, etc.

Throughout 2020, DVEs with differing goals and perspectives exploited such events to promote, organize, conspire, and plot against ideological opponents and other targets. DVEs’ efforts to engage in violence at lawful gatherings will probably increase throughout 2021, as some DVEs perceive increased socio-political pressures. Such perceived pressures may stem from, but not be limited to, one or more of the following factors:

- The potential for shifts in various policies many DVEs may perceive to oppose or threaten their ideological goals and agendas or feed into existing narratives many DVEs subscribe to regarding the U.S. government’s exercise of power, influence, and initiatives; possibly including firearm legislation, the easing of immigration restrictions, and new limits on the use of public land.
- Ongoing narratives by DVEs that the 2020 General Election was illegitimate, or fraudulent, and the subsequent belief its results should be contested or unrecognized.
- Some DVEs’ discontent with renewed measures to mitigate the spread of COVID-19, the ordered dissemination of COVID-19 vaccinations, and the efficacy and/or safety of COVID-19 vaccinations.

⁹¹ BofA-HJUD-00000040 (email from FBI to BoA “attach[ing] LIR titled ‘Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach’” and referencing the report as an “addition to” the “daily *Overnight News*” intelligence shared via the DSAC portal) (emphasis added); *see also* BofA-HJUD-00000041, 42, 43 (including LIR report); USBANK_HJC_000037.

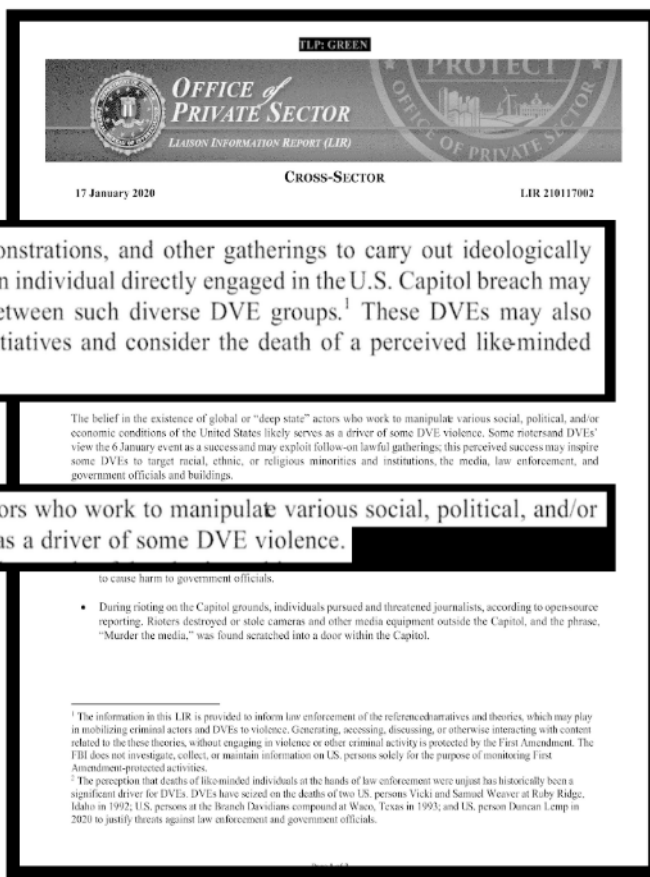
⁹² *Id.* at 41.

⁹³ *Id.*

⁹⁴ *Id.* at 42.

⁹⁵ *Id.*

In other words, according to the FBI, an American citizen’s opposition to firearm regulations, open borders, or COVID-19 lockdowns and vaccine mandates—all of which are viewpoints protected by the First Amendment to the Constitution—“feed into” an “existing narrative many DVEs subscribe to regarding the U.S. government’s exercise of power.”⁹⁶ Put another way, expressing a belief in the existence of the “deep state,” support for typical conservative policies with respect to firearms or immigration, or doubt about the conventional narrative, may result in an individual being labeled by the FBI as a “DVE Actor” and “Likely to Pose [an] Increasing Threat at Lawful Protests, Rallies, [and] Demonstrations. . .”⁹⁷ It is disturbing that the most powerful law enforcement agency in the country would consider views widely held by millions of Americans as the signs of domestic violent extremism. Worse yet, the federal government endorsed this determination with its partners by sharing the report with the largest and most powerful for-profit corporations in the world to alert them about potential “threat[s]” from the people it describes.⁹⁸



DVEs may exploit future lawful protests, rallies, demonstrations, and other gatherings to carry out ideologically motivated violence and criminal activity. The death of an individual directly engaged in the U.S. Capitol breach may serve to galvanize DVEs and increase collaboration between such diverse DVE groups.¹ These DVEs may also perceive the event as a step toward achieving their initiatives and consider the death of a perceived like-minded individual as an act of martyrdom.²

The belief in the existence of global or “deep state” actors who work to manipulate various social, political, and/or economic conditions of the United States likely serves as a driver of some DVE violence. Some rioters and DVEs view the 6 January event as a success and may exploit follow-on lawful gatherings; this perceived success may inspire some DVEs to target racial, ethnic, or religious minorities and institutions, the media, law enforcement, and government officials and buildings.

The belief in the existence of global or “deep state” actors who work to manipulate various social, political, and/or economic conditions of the United States likely serves as a driver of some DVE violence.

to cause harm to government officials.

- During rioting on the Capitol grounds, individuals pursued and threatened journalists, according to open-source reporting. Rioters destroyed or stole cameras and other media equipment outside the Capitol, and the phrase, “Murder the media,” was found scrawled into a dove within the Capitol.

¹ The information in this LIR is provided to inform law enforcement of the referenced narratives and theories, which may play in mobilizing criminal actors and DVEs to violence. Generating, accessing, discussing, or otherwise interacting with content related to these theories, without engaging in violence or other criminal activity is protected by the First Amendment. The FBI does not investigate, collect, or maintain information on U.S. persons solely for the purpose of monitoring First Amendment-protected activities.

² The perception that deaths of like-minded individuals at the hands of law enforcement were unjust has historically been a significant driver for DVEs. DVEs have seized on the deaths of two U.S. persons Vicki and Samuel Weaver at Ruby Ridge, Idaho in 1992; U.S. persons at the Branch Davidians compound at Waco, Texas in 1993; and U.S. person Duncan Lemp in 2020 to justify threats against law enforcement and government officials.

Astoundingly, the FBI’s report was an incredibly tone-deaf exercise of government gaslighting. In a clear example, the report deplored the belief in the existence of a “deep state” as

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.* at 40; see also FEDERAL BUREAU OF INVESTIGATION, OFFICE OF PRIVATE SECTOR, PRIVATE SECTOR ENGAGEMENT PROGRAMS AND INITIATIVES.

indicative of domestic violent extremism.⁹⁹ Ironically, the report itself was likely shared through a secret, government-run information-sharing portal that is only accessible to the government and some of the largest “for-profit companies” in the world.¹⁰⁰ To put a finer point on this hypocrisy, the report defines “deep state actors” as those who “work to manipulate various social [and] political” conditions.¹⁰¹ In the same breath, the report acknowledges the existence of “removal efforts” of social media platforms against potential domestic violent extremists.¹⁰² In effect, the report admits that social media companies are engaging in censorship—or the “manipulat[ion]” of speech—while labeling those who believe in the existence of such manipulation as potential domestic terrorists.¹⁰³

ii. The FBI commandeered financial institutions’ databases to conduct sweeping searches without an individualized nexus to particularized criminal conduct.

The Fourth Amendment to the Constitution protects against unreasonable searches and seizures by the federal government.¹⁰⁴ The founders likely would have never imagined a circumstance in which the federal government would conduct mass surveillance of Americans’ financial data. Yet, the information available to the Committee and Select Subcommittee shows how federal law enforcement sought sweeping searches of financial institutions’ customer databases without legal process, and even circulated materials instructing financial institutions on how to conduct those searches using Merchant Category Codes (MCCs) and other materials to alert them to customers likely to be associated with conservative political views.

1. The FBI contacted Bank of America directly and provided extremely broad search terms for querying its database and sharing any potential matches with federal law enforcement.

At 9:56 a.m. on January 15, 2021, an FBI official emailed BoA with the subject line “upcoming SAR product idea/brainstorming and check-in with you both.”¹⁰⁵ In the body of that email, the FBI official wrote that “[i]f either or both of you have time this morning to discuss SARs [Suspicious Activity Reports] and a couple ideas, that would be great.”¹⁰⁶

⁹⁹ *Id.* at 41.

¹⁰⁰ See BofA-HJUD-00000040, *supra* note 91; see also, e.g., BofA-HJUD-00000054 (Jan. 28, 2021, email from DSAC Portal to BoA (showing the DSAC portal distributing intelligence products titled “*Overnight News* – January 28, 2021” and suggesting distribution of the Liaison Information Report via the DSAC portal.) (emphasis added).

¹⁰¹ BofA-HJUD-00000041.

¹⁰² BofA-HJUD-00000041.

¹⁰³ Compare BofA-HJUD-00000041 with BofA-HJUD-00000042.

¹⁰⁴ U.S. Const. amend. IV.

¹⁰⁵ BofA-HJUD-00000001.

¹⁰⁶ *Id.*

From: [REDACTED] (FBI) [REDACTED]@fbi.gov]
 Sent: 1/15/2021 9:56:49 AM
 To: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
 Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

If either or both of you have time this morning to discuss SARs and a couple ideas, that would be great.

I will be on my cell this morning.

[REDACTED]

In a subsequent email just a couple of hours later, the FBI told BoA “thanks for the very quick communication/response over the phone this morning . . . [t]o recap our morning call, we [FBI] are prepared to action **[immediately]** the following thresholds,” supplying BoA with broad search thresholds for querying the financial transactions of its customers for potential matches.¹⁰⁷ The FBI explained that it “is interested in all financial relationships” of any BoA customer transacting in Washington, D.C. and that made “ANY historical purchase” of a firearm, or that had purchased a hotel, Airbnb, or airline travel within a given date range.¹⁰⁸

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:

- o 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].
 - Secondly, 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.

¹⁰⁷ BofA-HJUD-00000002.

¹⁰⁸ *Id.*

Just one day later, BoA confirmed to the FBI that it was “doing some work around the parameters we discussed and should have something out before the end of the weekend.”¹⁰⁹ BoA delivered as promised. On the evening of Sunday, January 17, 2021, BoA replied to the FBI indicating that it had compiled a product that was responsive to the FBI’s parameters, explaining “you [FBI] should have an email from [redacted]@bofa.com with our filing on the parameters you discussed with [redacted] last week.”¹¹⁰

From: [redacted]@bofa.com
Sent: 1/17/2021 7:54:23 PM
To: [redacted]@fbi.gov; [redacted]@fbi.gov
CC: [redacted]@bofa.com; [redacted]@bofa.com
Subject: RE: [SecMail:] secmail:RE: Follow-up

[redacted] -- you should have an email from [redacted]@bofa.com with our filing on the parameters you discussed with [redacted] last week.

Thanks,
[redacted]

[redacted]

From: [redacted]@fbi.gov [mailto:[redacted]@fbi.gov]
Sent: Saturday, January 16, 2021 11:26 AM
To: [redacted]@bofa.com>
Cc: [redacted]@bofa.com>; [redacted]@bofa.com>; [redacted]@fbi.gov
Subject: RE: secmail:RE: Follow-up

[redacted]

Great. Thanks. I will run with the info.

[redacted]

From: [redacted]
Sent: Sat, 16 Jan 2021 15:16:38 +0000
To: [redacted] (FBI)
Cc: [redacted]
Subject: Follow-up

Hi [redacted]

Following up from our conversation yesterday morning, we are doing some work around the parameters we discussed and should have something out before the end of the weekend.

¹⁰⁹ BofA-HJUD-00000197.

¹¹⁰ *Id.*

This massive search request, sent directly from the FBI to BoA, appears to have occurred via direct email, without any legal process or individualized criminal nexus.¹¹¹ As a result, a “filing” was created that was seemingly a “data dump” of BoA account information—reflecting potentially thousands of customers—that was turned over to the FBI.¹¹²

The Committee and Select Subcommittee requested, and subsequently subpoenaed, this “filing” from BoA.¹¹³ The Committee and Select Subcommittee also offered to accommodate BoA by allowing “redact[ions] to protect personal identifiable information.”¹¹⁴ Despite this, BoA declined to produce the requested documents, writing “[e]ven though a subpoena has now been issued, federal law, including the Anti-Money Laundering Act and the Bank Secrecy Act, together with their implementing regulations, still would prevent the Bank from disclosing certain documents.”¹¹⁵

While BoA has refused to provide the Committee and Select Subcommittee with its “filing on the parameters” it discussed and shared with the FBI, it is clear that the FBI was not interested in particularized criminal activity.¹¹⁶ Rather, the FBI cast a wide net with its search parameters and used BoA’s database to identify responsive accounts, creating a sprawling file of individuals whose financial accounts were flagged for federal law enforcement without any particularized allegation of engaging in federal criminal conduct. It is highly disturbing for any huge financial institution to comply with such a sweeping request from federal law enforcement and hand over its customers’ information without any legal process or regard for the privacy of its customers’ information.¹¹⁷

2. FinCEN, in coordination with a select group of financial institutions, shared Merchant Category Codes and politicized search terms and typologies for financial institutions to probe their databases for problematic accounts or transactions.

In addition to the sweeping requests from the FBI to financial institutions, FinCEN circulated materials to financial institutions containing instructions on how to search their databases and flag certain transactions using Merchant Category Codes (MCCs), typologies, and other key terms, phrases, or groups of concern. MCCs are used by “[p]ayment brands, issuers and acquirers . . . to categorize, track and restrict transactions” and can be used for “tax reporting, interchange promotion and gathering information about cardholder purchasing behavior.”¹¹⁸ MCCs, therefore, are a powerful tool for monitoring and restricting customer

¹¹¹ *See id.*

¹¹² *See id.*

¹¹³ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp. (Nov. 16, 2023).

¹¹⁴ *Id.* at 4.

¹¹⁵ Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Dec. 15, 2023) (discussing the Anti-Money Laundering Act and the Bank Secrecy Act as “prevent[ing] the Bank from disclosing certain documents”).

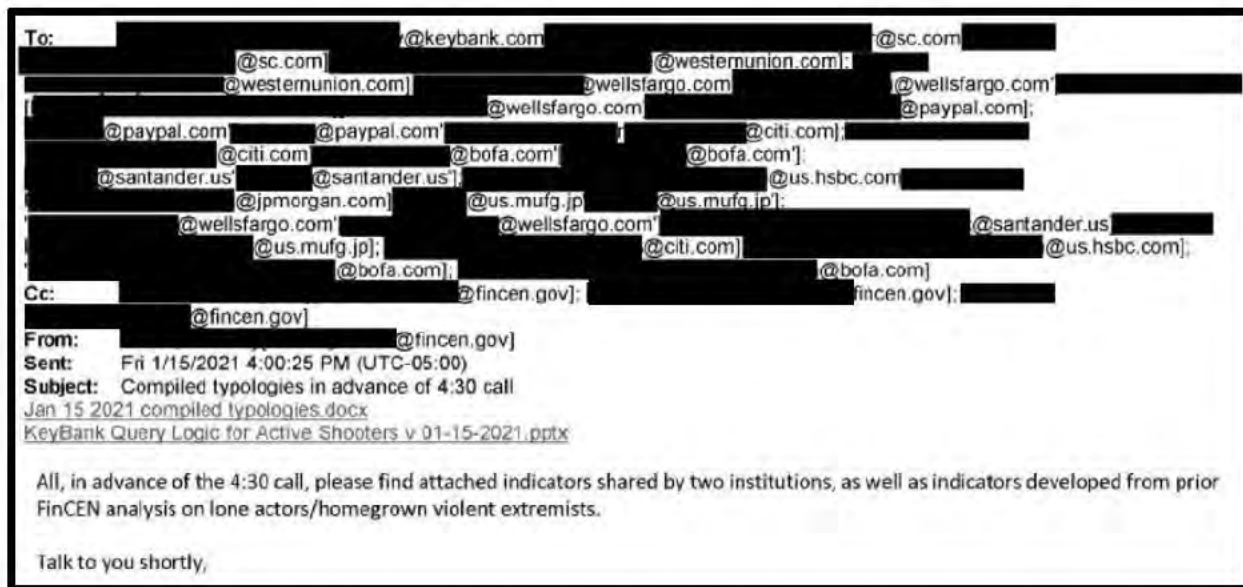
¹¹⁶ BofA-HJUD-00000002.

¹¹⁷ *See* BofA-HJUD-00000197; FEDERAL RESERVE STATISTICAL RELEASE, LARGE COMMERCIAL BANKS (2023).

¹¹⁸ *E.g.*, CITIBANK, MERCHANT CATEGORY CODES (2015), <https://www.citibank.com/tts/solutions/commercial-cards/assets/docs/govt/Merchant-Category-Codes.pdf>. For example, transactions related to “Motor Vehicle Supplies

purchases. The use of select MCCs and politicized search terms and phrases suggest a concerted effort to target a certain segment of the American population. Even worse, they show how federal law enforcement leveraged its relationship with financial institutions to search transactions and account records without legal process or the customers' knowledge or approval.

a. FinCEN provided financial institutions with politicized materials casting conservative points of view and lawful purchases as suspicious.



On January 15, 2021, at 4:00 P.M., FinCEN circulated two attachments to various financial institutions titled “Jan 15 2021 compiled typologies” and “KeyBank Query Logic for Active Shooters v. 01-15-2021.”¹¹⁹ These attachments provided financial institutions with suggested search terms—such as “AMERICA FIRST,” “TRUMP,” and “MAGA”—to use for identifying transactions that may be an indication “of involvement in riots or potential violence.”¹²⁰

and New Parts” may be identified with the MCC “5013” and transactions made at “Grocery Stores” may use the MCC “5411.”

¹¹⁹ HJC118_0000005 (showing email from FinCEN distributing “search terms” and “compiled typologies” of “extremism indicators” and “KeyBank Query Logic” PowerPoint slides as attachments to KeyBank, Standard Chartered, Western Union, Wells Fargo, Paypal, Citibank, Bank of America, Santander, HSBC, MUFG, and JPMorgan).

¹²⁰ HJC118_0000006.

1) Bank submission:

One of the things we've done is search Zelle payment messages for indications of involvement in the riots or potential violence. Here are the key words we used below to pull the data. [...] from our initial analysis "Storm the", "Capitol", "white power" and "Antifa" seem to be yielding the best results.

%PRESIDENT%
%PREZ%
%TRUMP%
%KAMALA%
%BIDEN%
%DIE%
%KILL%
%SHOOT%
%BLOW%
%GUN%
%DEATH%
%MURDER%
KRAKEN
ANTIFA
LAST SONS
OATH KEEPER
WHITE POWER
CAPITOL
STORM THE
CIVIL WAR
GROYPER ARMY
CAMP AUSCHWITZ
AMERICA FIRST
THREEPERS
MILITIA
CAPITAL
MAGA
PATRIOT
BOOGALOO
PROUD B%
CIVIL WAR
PELOSI
PENCE
Schumer

2) Lone Actor/Homegrown Violent Extremism Indicators (developed from prior FinCEN analysis)

- ✓ Long periods of account inactivity, or show normal usage, but in the months or years preceding an attack, a sudden surge or change in activity type.
- ✓ Sudden purchase of firearms, firearm parts and accessories, ammunition, tactical gear at outdoor supply stores, and purchases at shooting ranges not commensurate with previously known customer behavior.

In addition, the documents include a "prior FinCEN analysis" suggesting indicators of potential "Lone Actor/Homegrown Violent Extremism."¹²¹ Those indicators included, among other items, "frequent ATM withdrawals and wire transfers with no apparent economic or business purpose"; "transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose"; "purchases that appear excessive or unusual for hobbyist or other legitimate use"; "the purchase of books (including religious texts) and

¹²¹ HJC118_000006.

subscriptions to other media containing extremist views”; and “donations to organizations known to promote radicalism.”¹²²

- ✓ Frequent cash deposits of unknown origin, followed by debit or credit card purchases at retailers not commensurate with previously known customer purchase activity.
- ✓ Frequent ATM withdrawals and wire transfers with no apparent economic or business purpose.
- ✓ Sudden account closings, asset liquidations, and disbursements in days or weeks leading up to attacks.
- ✓ Life insurance policy purchases not commensurate with typical behavior for the type of account holder.
- ✓ Transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose or not commensurate with the previous travel history of the customer, for example, travel to high-risk areas or indirect flightpaths for no apparent legitimate reason.
- ✓ Purchases that appear excessive or unusual for hobbyist or other legitimate use.
- ✓ The purchase of pre-cursor chemicals, fireworks, or potential bomb-making equipment, for example, ammonium nitrate, citric acid, aluminum powder, triacetone triperoxide [TATP], potassium nitrate, red iron oxide, tannerite, lengths of piping, BB pellets, cell phones, and others.
- ✓ Purchases of international calling cards not commensurate with previously known customer behavior.
- ✓ The purchase of books (including religious texts) and subscriptions to other media containing extremist views.
- ✓ Donations to organizations known to promote radicalism.

As shown, the list, prepared by FinCEN, demonstrates that federal law enforcement is interested in scrutinizing otherwise lawful transactions such as “ATM withdrawals,” transportation-related expenses for “no apparent legitimate reason,” “donations to organizations known to promote radicalism,” and “the purchase of books (including religious texts) and subscriptions to other media containing extremist views.”¹²³ In other words, the federal government broadly enlisted financial institutions to flag certain kinds of purchases made by Americans that the government deemed to be unnecessary—*e.g.*, taking trips for “no apparent legitimate reason”—or extreme—*e.g.*, purchasing certain books or “religious texts.”¹²⁴ There is no indication in the documents that FinCEN recognized the serious civil liberty concerns associated with its demands or took any steps to protect Americans’ financial privacy.

In the same email, FinCEN also circulated a PowerPoint slide deck as an attachment, authored by KeyBank, titled, “KeyBank’s Query Logic for Active Shooters,” that “intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (‘Lone Wolves’).”¹²⁵ That slideshow showed in stark terms how federal authorities and financial institutions can weaponize MCCs to identify and target Americans using the financial system.

¹²² HJC118_0000007.

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ HJCSWFG_0000454.PPTX. at 2.

Active Shooter Detection – Intent of Query

- Intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (“Lone Wolves”).
- Assumes individuals are creatures of habit and tend to frequent and/or shop at the same places when buying the same or similar items, rather than purchasing the same thing at multiple merchants or vendors.
 - Looks for purchases at multiple merchants or vendors who sell weapons and/or ammunition over a shorter period of time.
- Looks for “bursts” of potential suspicious purchase activity, especially when activity not seen previously.
 - Run query periodically, using a rolling lookback period of 60 days.
- Focuses on credit / debit card transaction activity with merchant / vendor counterparties.
 - Looks at specific counterparty Merchant Category Classification Codes (MCC Codes) and distinct merchant IDs.
 - MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID.
 - No minimum dollar threshold for individual transactions.
 - Uses an iterative feedback loop process to build out and refine the exclusion and inclusion keyword lists (detailed in the next slides).
 - Limitations – Due to a lack of industry identifiers for counterparties for other transaction types, does not look at cash, check, ACH, or wire transactions at this time.
- SARs filed for public safety / law enforcement awareness purposes.
- **Alert Example** – John Doe makes 5 credit card purchases at 4 different gun shops, plus makes 4 charges at 3 gun ranges, spending \$3,000 on weapons-related transactions over a 5 week period. Doe does not appear to have any previous firearms purchases.

Classification: KeyCorp Confidential

1



The concern around the use of MCCs to sift through and flag certain purchases on behalf of federal law enforcement is well-documented. For example, in September of 2022, after being petitioned by Amalgamated Bank—an institution that leverages financial power to promote “sustainable organizations, progressive causes, and social justice”¹²⁶—the International Organization for Standardization (ISO) announced its intent to create a separate MCC for the sale of firearms in America with the unabashed support of gun control advocates.¹²⁷ That announcement sparked an outcry from many Americans who opposed ISO’s announcement out of fear that it would be used to track, harass, and limit firearm vendors’ and purchasers’ access to financial services.¹²⁸ As a result of the pressure, the program was reportedly put on pause.¹²⁹ However, the Committee and Select Subcommittee’s investigation has revealed that similar MCCs are already being weaponized against customers by financial institutions in collusion with federal law enforcement.¹³⁰

The KeyBank slide deck also included slides that provided financial institutions with search query logic terms and instructions on how to search through their transactions and accounts in order to “detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (‘Lone Wolves’).”¹³¹ These slides detail how financial institutions can wield MCCs, merchant IDs, and other keyword searches to monitor customer transactions for “suspicious” activity. As the previous slide

¹²⁶ AMALGAMATED BANK, <https://amalgamatedbank.com/who-we-are> (last visited Feb. 28, 2024).

¹²⁷ Andrew Sorkin, *Credit Card Issuers Join the Fight to Limit Mass Shootings*, N.Y. TIMES (Sept. 12, 2022).

¹²⁸ See, e.g., Letter from Rep. Elise Stefanik et. al, to Mr. Alfred F. Kelly, Chief Exec. Officer of Visa, Inc. (Sept. 14, 2022); see also J.D. Tuccille, *Credit Cards ‘Pause’ Efforts to Track Gun Purchases After Pushback*, REASON (Mar. 13, 2023).

¹²⁹ See J.D. Tuccille, *supra* note 128.

¹³⁰ See, e.g., HJCSWFG_0000454.PPTX.

¹³¹ HJCSWFG_0000454.PPTX. at 2.


explains, “MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID” and should not use any “minimum dollar threshold for individual transactions.”¹³² In other words, every transaction is assigned an MCC and financial institutions use these codes to search through customers’ financial history for any activity it deems “suspicious.” If it finds a possibly suspicious transaction, it can report that information to federal law enforcement by filing a SAR or similar report without the customer ever knowing about it.¹³³

Active Shooter Detection – Methodology 1 – Keyword EXCLUSION (Broad Focus)

- Transaction Population:** Query for credit / debit card purchases involving any of the following MCC codes:
 - 3484: Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - 3489: Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - 5091: Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - * Not universally recognized MCC code
 - 5099: Durable Goods, Not Elsewhere Classified
 - 5933: Pawn Shops
 - 5941: Sporting Goods Stores (largest sellers of firearms and ammunition)
 - 5999: Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - 7999: Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)
- Keyword EXCLUSION (Above transactions must EXCLUDE these keywords / Not exhaustive list):**

Amazon	Bowling	Fitness	Laundry	Roll	Tobacco
Angler	Casino	Food	LifeVantage	Scuba	Tonka
Archery	Card	Football	Linen	Shoe	Vape
Bait	Carquest	Gift Shop	Lodge	Skate	Vapor
Baseball	Cig	Golf	Low's	Ski	Victor/assacret
Bath & Body	Coffee	Google	Mercari (exact)	Smoke	Vitamin
Beauty	Comic	Graze	Metalace	Snorkel	Volleyball
Bicycle	Communication	Harris Teller	Music	Stovax	Water
Bike	Danbury Mint	Hockey	Party	Spirit Manufacturing	Wish.com (exact)
Billy Beatz	DirectTV	Home Depot	PayPal (unless it also includes "Gun")	Square (exact)	Yoga
Binge	Dive	Hoops	Pizza	Storage	Zur
Boat	Ebay	Hospital	Post	Swim	Zully (exact)
Body	Engineering	Indeod	Print	Tackle	
BodySolid	Essex.com	iTunes	Culver	Tan	
Boutique	Farm	Jewel	Resort	Tee	
Bow	Fish	Johnson Hill		Tennis	
- During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, AND
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, AND
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, AND
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.

Classification: KeyCorp Confidential



As the KeyBank slide demonstrates, financial institutions often use MCCs to query and review transactions for potentially suspicious activity. This slideshow directs particular concern to firearm-related purchases, lawful or otherwise, under the guise of detecting DVEs.¹³⁴ It reveals that financial institutions can use special MCCs to identify certain purchases for review, including “3484: Small Arms,” “3489: Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30mm),” “5091: Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales),” “5099: Durable Goods, Not Elsewhere Classified,” “5933: Pawn Shops,” “5941: Sporting Goods Stores (largest sellers of firearms and ammunition),” “5999: Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers),” and “7999: Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges).”¹³⁵

¹³² *Id.*

¹³³ See 31 U.S.C. § 5318(g)(3)(A); see also 12 U.S.C. § 3403(c); 31 C.F.R. § 1020.320(a)(1), (e).

¹³⁴ HJCSWFG_0000454.PPTX, at 3.

¹³⁵ *Id.*; See also KEYBANK, KEY2 PURCHASE MCC,

https://www.key.com/content/dam/kco/documents/businesses_institutions/Key2Purchase_MCC.pdf (last visited Jan. 22, 2024). The Committee and Select Subcommittee note that KeyBank omits use of MCCs 3484, 3489, and 5091 in its publicly available MCC list.

Active Shooter Detection – Methodology 2 – Keyword INCLUSION (Narrow Focus)

- **Transaction Population:** Query for credit / debit card purchases involving any of the following MCC codes:
 - **3484:** Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - **3489:** Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - **5091:** Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns safes)*
 - **5099:** Durable Goods, Not Elsewhere Classified
 - **5933:** Pawn Shops
 - **5941:** Sporting Goods Stores (largest sellers of firearms and ammunition)
 - **5999:** Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - **7999:** Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)
- **Keyword INCLUSION (Above transactions must INCLUDE one of these keywords / Not exhaustive list):**

▪ Academy.com	▪ Cabela's	▪ Edge Works Manufacturing	▪ HarrisBipods.com	▪ NorthShoreFirearms.com	▪ SOG International
▪ Aere Precision	▪ CalLegalMags.com	▪ Ekilife Supply	▪ ImpactGuns.com	▪ Noveske.com	▪ SouthernOhioGun.com
▪ AimSurplus	▪ CarrierComp.com	▪ EkilifeWorks.com	▪ JP Enterprises	▪ NTCTrading.net	▪ SpikesTactical.com
▪ AnarchyOutdoors.com	▪ ChattanoogaShooting.com	▪ EkilifeDefense.com	▪ JPRifles.com	▪ Numrich Gun Parts	▪ SportsmanGuide.com
▪ Anderson Manufacturing	▪ ChesperThunDist.com	▪ FreedomMerchants.com	▪ JESurplus.com	▪ OpticsPlanet.com	▪ STIGuns.com
▪ AR-15.co	▪ ClassicCollectonFirearms.com	▪ Gander Mountain	▪ KAKIndustry.com	▪ OregonRifleworks.com	▪ STI International
▪ AR15.com	▪ ClassicCollectonFirearms.com	▪ Gaiwala.com	▪ Kawambit.com	▪ ParkerMountainMachine.com	▪ Taccom
▪ B & T Industries	▪ CopcoDistributing.com	▪ GhostGuns.com	▪ KingFirearmsAndMore.com	▪ RobertsonTradingPost.com	▪ Taccom3G.com
▪ Backcountry World	▪ DawsonPrecision.com	▪ GhostGunnet.com	▪ KingFirearmsOnline.com	▪ Ruger	▪ TaccomCanada.com
▪ Bass Pro Shop	▪ DeltaDefense.com	▪ Glock	▪ MidwayUSA.com	▪ S&W	▪ TargetSportsUSA.com
▪ Blade HQ	▪ DeltaTeamTactical.com	▪ Gova.com	▪ M&MTargets.com	▪ Sarcocinc.com	▪ WC Wolf Co.
▪ BladeOps.com	▪ Dick's Sporting Goods	▪ GRKnives.com	▪ Mike Gibson Manufacturing	▪ ShootingTargets7.com	▪ WideOpenSpaces.com
▪ Bladefire	▪ DillonPrecision.com	▪ GrindGuns.com	▪ Mike's Gun Shop.net	▪ SIG Sauer	▪ WittMachins.net
▪ Bladefire.com	▪ DLTTrading.com	▪ GrindGuns.com	▪ Mike's Gun and Pawn	▪ SilencerShop.com	
▪ BuyItGunstocks.com	▪ DSG (Dick's Sporting Goods)	▪ GunBroker.com	▪ MileHighShooting.com	▪ Silent Precision	
▪ BravoCompanyUSA.com	▪ Dunkeilbergers.com	▪ GunPartsCorp.com	▪ NewFrontierArmory.com	▪ SMKW.com	
▪ Brownells	▪ E-Sarcolinc.com	▪ GunSprings.com		▪ SnipeCentral.com	
▪ Browning					
- **During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, **AND**
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, **AND**
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, **AND**
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.

Classification: KeyCorp Confidential



These MCCs were also used to target transactions involving specific retailers and may have been flagged for federal law enforcement despite having no nexus to criminal activity.¹³⁶ As the KeyBank slide shows, transactions involving any of the previously named MCCs can be narrowed using additional keywords. Those keywords include transactions from retail stores like “Dick’s Sporting Goods,” “Gander Mountain,” “Bass Pro Shop,” “Cabela’s,” “Backcountry World,” “TargetSportsUSA.com,” “AR15.com,” “MidwayUSA,” among many others.¹³⁷

Another one of the KeyBank slides, circulated by FinCEN, directed financial institutions to other transactions of interest, listing such “red flags” that “[i]nvestigators may wish to consider” when “reviewing financial accounts” and included:

- “unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction”;
- “any recent purchases of counter-surveillance equipment”;
- “any recent purchases of covert / secure communications equipment” such as “Virtual Private Networks (VPNs), online gaming, prepaid phones / calling cards”;
- “any recent rental of storage facilities”;
- “other excessive transactions” such as “hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms”;
- “excessive ATM, Prepaid Cards, Person-to-Person, or Virtual Currency transactions”;
- “recent life insurance purchases and/or bank account closures”;
- “any life stressor indicators” such as “no payroll deposits”;

¹³⁶ HJCSWFG_0000454.PPTX. at 4.

¹³⁷ *Id.*


- “recent excessive legal / medical expenses (legal / family status or health challenges)”;
- and whether the individual is unemployed, was “recently fired or laid off,” has “delinquent / excessive debt,” or has “social media posts of concern.”¹³⁸

Of course, none of these transactions standing alone are unlawful—in fact, many are indicative of constitutionally protected political or religious activity.

Active Shooter Detection – Additional Red Flags to Consider

When Investigators are reviewing financial accounts, besides alerted transactions, other factors Investigators may wish to consider:

- Is the alerted transaction activity consistent with previous activity, or has it begun recently?
- Unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction?
- Any recent purchases of counter-surveillance equipment?
- Any recent purchases of covert / secure communications equipment?
 - Virtual private networks (VPNs), online gaming, prepaid phones / calling cards, etc. transactions?
- Any recent rental of storage facilities?
- Other excessive transactions, especially if not consistent with previous activity?
 - Hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms, etc.
- Excessive ATM, Prepaid Cards, Person-to-Person (P2P), or Virtual Currency transactions?
- Any recent life insurance purchases and/or bank account closures?
- Any life stressor indicators?
 - Recent excessive legal / medical expenses (legal / family status or health challenges)?
 - No payroll deposits? Unemployed? Recently fired or laid off?
 - Delinquent / excessive debt?
- Any social media posts of concern?

Classification: KeyCorp Confidential 

Similarly, on January 16, 2021, FinCEN circulated additional slides prepared by the Global Financial Crimes Division (GFCD) at MUFG Bank, the largest bank of Japan, to other financial institutions and that included a “list of subjects of interest and high-level typologies.”¹³⁹ That slide revealed typologies for review as they relate to the events of “1/6” and included a broad scope of credit, debit, and ATM transactions, suggesting a look-back period ranging from November 3, 2020, to January 12, 2021.¹⁴⁰ These typologies include otherwise lawful activity such as “use of business cards (not held by tactical or security firms) for the purchase of arms / ammo,” “transfers to GiveSendGo or other crowdsourcing sites,” “purchasing of gift cards; Use of debit cards for Crypto,” and “transactions in or near capitols or state capitols at/around 1/6.”¹⁴¹

¹³⁸ HJCSWFG_0000454.PPTX. at 5.
¹³⁹ HJCSWFG_0000003 (email from FinCEN distributing slide to KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase); see also HJCSWFG_0000007.
¹⁴⁰ *Id.*
¹⁴¹ *Id.*

GFCD Intelligence & Analytics Data Insights and Analytics

A Strictly Confidential
Customer Information

Typologies for review as they relate to the events of 1/6/20

Scope: Transactions pulled from 11/3 – 1/12: ATM, CREDIT, DEBIT, with expanded reviews where needed.

#	Typology
1	MCC Codes that, when taken together, demonstrate travel: ex. hotel, rental car, & gas, AND Mileage increasingly further from cardholder's home
2	Cardholder purchases at gun-ammo, sporting goods stores, etc., that demonstrate increases in volume, value, or velocity above average and/or a high % relative to cardholder's available credit. Transactions that contain keyword list matches: a) potential target events, locations, or individuals b) names:
3	i: of those arrested at demonstrations / riots ii: of key leadership in organizations c) code terms and calls to action d) precursor elements to IEDs and firearms
4	Transactions in or near capitols or state capitols at/around 1/6
5	Multiple cards used by one person, for the purchasing of fire arms/ammo etc.
6	Use of business cards (not held by tactical or security firms) for the purchase of arms / ammo
9	Transfers to GiveSendGo or other crowdsourcing sites
10	Purchasing of gift cards; Use of debit cards for Crypto
11	Over/under invoicing for merchant codes at gun clubs with other vendor services (i.e., large transactions for an individual at a snack bar)

 MUFG

NOTE: DIA plans on looking at these typologies holistically, that is no single hit may warrant escalation but more than one could.

DIA plans on, where possible, pulling transaction details for Credit, ATM, and DEBIT card activity.

DIA will look to sort for these typologies via in person vs. online purchases

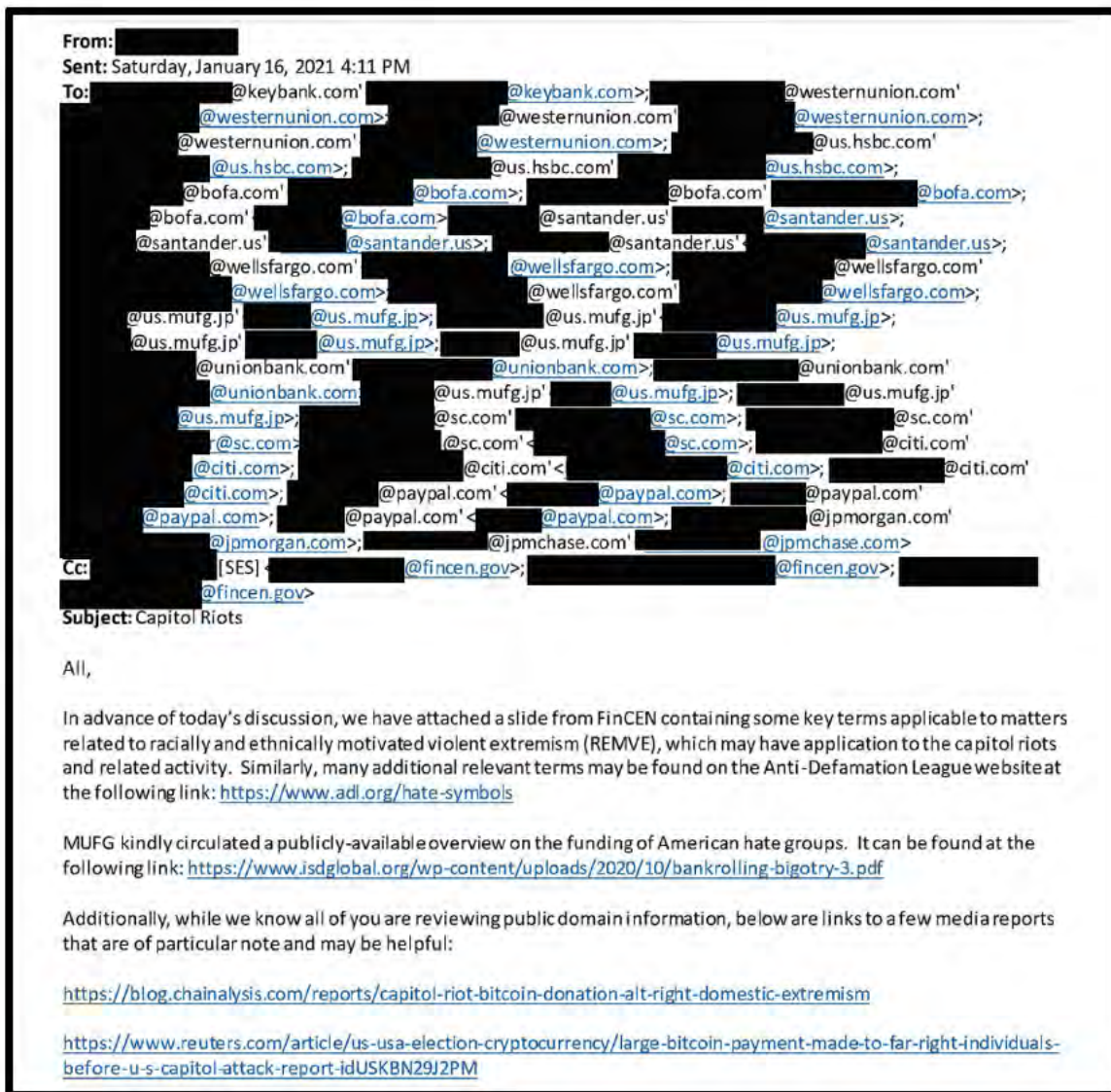
The condition and contents of data may dictate that DIA will have to alter these typologies, abandon these typologies, and / or adopt new typologies

Consequently, account information and transactions meeting any of the eleven “typology” criteria may have been flagged and shared with federal law enforcement as being “suspicious.” The slide is another clear example that these typologies were not necessarily evidence of criminal activity, but that were nonetheless scrutinized and potentially shared with federal law enforcement. Unfortunately, the use of MCC search parameters were not the only kinds of typologies and transactions that FinCEN was interested in. FinCEN also circulated politicized materials to financial institutions for monitoring their databases for certain “hate groups” and other “key terms.”¹⁴²

¹⁴² HJCSWFG_0000004 (email from FinCEN sharing hyperlinks to KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase).

b. FinCEN shared a “hate symbols” database and a report on the funding of American “hate groups” to financial institutions.

On January 16, 2021, FinCEN circulated another email to financial institutions “in advance of today’s discussion.”¹⁴³ That email included links to “key terms applicable to matters related to racially and ethnically motivated violent extremism, which may have application to the capitol riots and related activity.”¹⁴⁴ In addition, the email included a hyperlink to “relevant terms” from the Anti-Defamation League website and a hyperlink to a “publicly-available overview on the funding of American hate groups.”¹⁴⁵ The first hyperlink was to a database of “Hate Symbols” indexed by the Anti-Defamation League (ADL)—a notorious anti-conservative activist group—and the second was to a report authored by the Institute for Strategic Dialogue



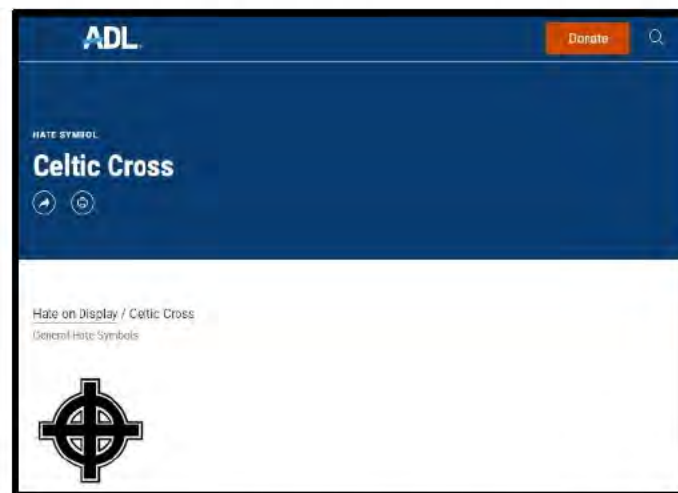
¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

(ISD) titled “Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups.”¹⁴⁶

In recent years, ADL has become significantly more left-wing and taken an aggressively anti-conservative stance. For example, the “Hate Symbols” database maintained by ADL and circulated by FinCEN to financial institutions treats “Anti-Antifa Images,” the “Celtic Cross,” the “Okay Hand Gesture,” “Pepe the Frog,” and “White Lives Matter,” as hate symbols.¹⁴⁷ It should alarm Americans that FinCEN approved of and distributed a link to a database that considers symbols of faith such as the Christian Celtic Cross and other images opposing Antifa—a violent left-wing anarchist group—as hate symbols. This practice is reminiscent of the FBI’s disdain for “Radical Traditionalist Catholics,” and the FBI’s reliance on the Southern Poverty Law Center—another far-left activist group—as an authoritative source on the Catholic Church.¹⁴⁸



FinCEN also circulated a hyperlink to a report authored by the ISD. The ISD is a left-wing organization that holds itself out as an “independent” monitor of “disinformation” that promotes the censorship of speech it decries as false or extreme.¹⁴⁹ FinCEN’s distribution of the ISD report amounts to an approval of its content, its methods, and its conclusions. Such an endorsement is concerning because the ISD report labels and demonizes various right-of-center groups in America as “hate groups.”¹⁵⁰ For example, the ISD’s report incorrectly characterizes several conservative groups such as the Center for Immigration Studies, Numbers USA, the

¹⁴⁶ ADL, HATE ON DISPLAY™ HATE SYMBOLS DATABASE, <https://www.adl.org/resources/hate-symbols/search> (last visited Feb. 28, 2024); Institute for Strategic Dialogue, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, ISD at 9 (Oct. 27, 2020).

¹⁴⁷ ADL, HATE ON DISPLAY™ HATE SYMBOLS DATABASE, <https://www.adl.org/resources/hate-symbols/search> (last visited Feb. 28, 2024).

¹⁴⁸ See STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON THE FBI’S BREACH OF RELIGIOUS FREEDOM: THE WEAPONIZATION OF LAW ENFORCEMENT AGAINST CATHOLIC AMERICANS 5 (Comm. Print 2023).

¹⁴⁹ Institute for Strategic Dialogue, <https://www.isdglobal.org/about/> (last visited Feb. 28, 2024); see also Letter from Rep. Michael T. McCaul, Chairman, H. Foreign Aff. Comm., to Hon. Antony J. Blinken, Secretary of St. (May 1, 2023).

¹⁵⁰ Institute for Strategic Dialogue, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, ISD (Oct. 27, 2020).

Alliance Defending Freedom, along with several others, as “hate groups.”¹⁵¹ In fact, the ISD’s report draws a false equivalency between certain conservative civil society groups and the American Nazi Party and the Knights of the Ku Klux Klan, suggesting FinCEN views them equally.¹⁵² Still, FinCEN circulated the ISD report to some of the largest financial institutions in the world, including the very financial institutions that are likely responsible for providing financial services to many of the listed “hate groups,” without regard for the chilling effect it would have on protected speech and its potential to be weaponized against the groups by financial institutions.

¹⁵¹ *Id.* at 9.

¹⁵² *Id.*

Table 2 Overview of hate groups studied

Anti-immigrant**Organisations**

- Center for Immigration Studies
- Dustin Inman Society
- Federation for American Immigration Reform
- Numbers USA
- Oregonians for Immigration Reform
- ProEnglish
- The Remembrance Project
- We The People Rising

Anti-LGBTQ+**Organisations**

- Pass the Salt Ministries
- All Scripture Baptist Church
- Alliance Defending Freedom
- American College of Pediatricians
- American Family Association
- American Vision
- Center for Family and Human Rights
- Chaldeon Foundation
- Church Militant and St Michael's Media
- Eagle Forum
- Family Research Council
- Family Watch International
- Liberty Counsel
- MassResistance
- National Organization for Marriage
- New Independent Fundamental Baptist Network
- Pacific Justice Institute
- Ruth Institute
- Westboro Baptist Church
- World Congress of Families

Anti-Muslim**Organisations**

- Act for America
- American Freedom Defense Initiative
- Center for Security Policy
- Clarion Project
- David Horowitz Freedom Center
- The United West

Militia or street protest**Organisations**

- American Patriots USA
- American Revolution 2.0
- Patriot Prayer
- Patriot Wave
- Proud Boys
- Rise Above Movement
- Washington Three Percenters
- Oath Keepers

White nationalist**Organisations**

- America First Students
- American Freedom Party
- American Guard
- Groypers – Nick Fuentes
- New Jersey European Heritage Association
- Patriot Front
- VDARE
- Identity Dixie
- League of the South

White supremacist**Organisations**

- American Identity Movement (formerly Identity Evropa)
- American Nazi Party
- American Renaissance, website of New Century Foundation
- Atomwaffen Division
- Bowl Patrol or Bowl Gang
- Feuerkrieg Division (international)
- Keystone United
- Knights of the Ku Klux Klan
- Legion of St. Ambrose
- National Alliance
- National Socialist Movement
- National Justice Party
- Northwest Front
- NSC 131
- Order 15
- Shield Wall Network
- The Base
- Vorherrschaft Division
- Kingdom Identity Ministries

Black supremacist**Organisations**

- Nation of Islam

Holocaust denial**Organisations**

- Institute for Historical Review

Misogynist**Organisations**

- A Voice for Men

C. FinCEN used financial institutions to monitor and report on accounts involved in crowdfunding for conservative events.

On January 18, 2021, FinCEN circulated a “list of crowdfunding sites” that “[p]eople have been observed using to post an event and sell tickets including bus tickets to the

demonstrations.”¹⁵³ In that email, FinCEN explained that financial institutions could be alerted to such customer transactions using the reference “EB [the EVENT] with the phone number,” adding as an example “EB MARCH FOR TR.”¹⁵⁴ In other words, FinCEN was soliciting and encouraging financial institutions to report on the accounts of any persons involved in crowdfunding events or demonstrations in support of President Trump.



As shown in the email, FinCEN did not provide any indication linking crowdfunding for conservative events to criminal activity.¹⁵⁵ Simply purchasing a ticket to the event was enough for FinCEN to consider this activity as suspicious. It is clear that FinCEN was comfortable with

¹⁵³ HJCSWFG_0000533 (email from FinCEN to KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase).

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

casting the selling of “bus tickets to the demonstrations” as suspicious without articulating any basis for believing such demonstrations might be unlawful.¹⁵⁶ However, the weaponization of crowdfunding against conservative movements is not new.¹⁵⁷ For example, GoFundMe removed fundraisers associated with the “Freedom Convoy,” a group protesting COVID-19 mandates internationally, and removed fundraisers on its platform supporting the legal defense of Kyle Rittenhouse while leaving fundraisers for Antifa militants and Black Lives Matter rioters untouched on the platform.¹⁵⁸ FinCEN’s incursion into the crowdfunding space represents a trend in the wrong direction and a threat to American civil liberties.

D. FinCEN circulated a KeyBank-created “Appendix” of “Domestic Extremist Groups” to other financial institutions.

FinCEN also distributed an additional slide, prepared by another financial institution, via email to other financial institutions.¹⁵⁹ The slide is an “Appendix” that labels certain groups as “Domestic Extremist,” including “American Border Patrol,” “Anti-Abortion (violent),” “Anti-Government,” the “Center for Immigration Studies,” and the “Center for Security Policy,” among many others.¹⁶⁰ By sharing this slide prepared by KeyBank, FinCEN endorsed a listing of groups it considered “domestic extremist.”

CONCLUSION

The decline of cash and the rise of digital payments and e-commerce platforms has provided financial institutions with more insight and influence over the financial system than ever before. In fact, very little financial activity occurs beyond the purview of modern financial institutions. As a result, these financial institutions often act as arms of federal law enforcement as they work in coordination with federal law enforcement to identify what transactions and other information is “suspicious” enough to be reported. Other times, law enforcement uses backchannel discussions to commandeer financial institutions’ databases in order to collect Americans’ data and build a profile of any “typology” it deems “suspicious.” When working together, these two parties wield a tremendous amount of influence and power over the American financial system with almost no oversight of their partnership and no possibility for recourse when that system is abused at the cost of victims who have been wrongfully targeted by the secret information-sharing network.

As this investigation shows, greater scrutiny of the partnership between federal law enforcement and financial institutions is warranted. When “Big Banks” and “Big Government” collude to violate American civil liberties, Congress has a responsibility to step in. Thanks to the brave whistleblower testimony that brought it to light, what started as an investigation into alarming information-sharing between Bank of America and the FBI without legal process has

¹⁵⁶ *Id.*

¹⁵⁷ See, e.g., Ryan King, *Five times GoFundMe shut down conservative fundraisers*, WASH. EXAMINER (Feb. 7, 2022).

¹⁵⁸ See Douglas Blair, *GoFundMe’s Sordid History of Censorship of Conservative Causes*, DAILY SIGNAL (Feb. 9, 2022).

¹⁵⁹ HJCSWFG_0000549 (email from FinCEN sharing slide with KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase).

¹⁶⁰ HJCSWFG_0000550.PPTX.

exposed what appears to be an even greater state of financial surveillance and weaponization. From targeting customers and transactions that shop at Bass Pro Shop or Cabela's using MCCs, to profiling customers with "typologies" that cast the purchase of religious texts and other donations to organizations that promote "radicalism" as indicative of "Homegrown Violent Extremism," federal law enforcement has overstepped its bounds.

As this investigation continues, the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government will continue to conduct oversight of the state of financial surveillance, targeting, and the vulnerabilities of Americans' data. Secret information-sharing portals and backchannel discussions outside the normal course of legal process pose serious risks to the nation. Larger questions remain regarding how the information shared between federal law enforcement and financial institutions was acted upon, and the ongoing extent of the financial surveillance. The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government remain committed to answering those questions and upholding the civil liberties of Americans.

Appendix

Date: Friday, January 29 2021 08:31 PM

Subject: [EXTERNAL] Capitol Riots Investigations

From: [REDACTED]@fbi.gov >

[REDACTED]@jpmchase.com > [REDACTED]@citi.com >; [REDACTED]
[REDACTED]@paypal.com > [REDACTED]@wellsfargo.com >
To: [REDACTED]@us.hsbc.com >; [REDACTED]@sc.com >; [REDACTED]
[REDACTED]@bofa.com >; [REDACTED]@usbank.com >; [REDACTED]
[REDACTED]@barclays.com >; [REDACTED]@jpmchase.com >
[REDACTED]@schwab.com >;

CC: [REDACTED]@fbi.gov >;

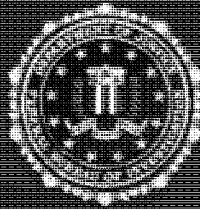
Good afternoon all,

For the past several months I have been working at our Washington Field Office under [REDACTED] who I believe most of you met while [REDACTED] was serving as the [REDACTED]. As the dust begins to settle here after the events of January 6th, [REDACTED] would like to hold a call with the goal of identifying the best approach to information sharing, both strategic and operational, related to the Capitol Riots. In the hopes of moving forward together quickly, we have set aside time at 2:30pm on Tuesday, February 2nd for this discussion. I will be sending out dial-in information first thing Monday and hope you, or someone from your team, is available to participate.

Thanks and have a great weekend!

[REDACTED]

[REDACTED]
Special Assistant to [REDACTED]
Federal Bureau of Investigation
Washington Field Office
[REDACTED]



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CROSS-SECTOR

17 January 2020

LIR 210117002

Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach

References in this LIR to any specific commercial product, process or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service or corporation on behalf of the FBI.

The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and National Counterterrorism Center (NCTC) prepared this LIR to alert private sector partners that the 6 January 2021 violent breach by suspected domestic violent extremists (DVEs) into the U.S. Capitol Building may serve as a driver for a diverse set of DVEs.

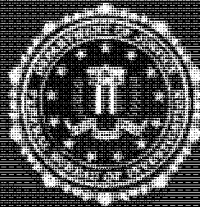
DVEs may exploit future lawful protests, rallies, demonstrations, and other gatherings to carry out ideologically motivated violence and criminal activity. The death of an individual directly engaged in the U.S. Capitol breach may serve to galvanize DVEs and increase collaboration between such diverse DVE groups.¹ These DVEs may also perceive the event as a step toward achieving their initiatives and consider the death of a perceived like-minded individual as an act of martyrdom.²

The belief in the existence of global or “deep state” actors who work to manipulate various social, political, and/or economic conditions of the United States likely serves as a driver of some DVE violence. Some rioters and DVEs’ view the 6 January event as a success and may exploit follow-on lawful gatherings; this perceived success may inspire some DVEs to target racial, ethnic, or religious minorities and institutions, the media, law enforcement, and government officials and buildings.

- An individual who traveled to Washington, D.C. engaged in lawful protests, illegally entered the U.S. Capitol Building, and was shot and killed by law enforcement personnel.
- Some participants at the Capitol displayed insignias used or adopted by a range of DVEs. Nooses and plastic restraints were carried or stationed at or near the Capitol by some rioters, possibly to demonstrate their intent to cause harm to government officials.
- During rioting on the Capitol grounds, individuals pursued and threatened journalists, according to open-source reporting. Rioters destroyed or stole cameras and other media equipment outside the Capitol, and the phrase, “Murder the media,” was found scratched into a door within the Capitol.

¹ The information in this LIR is provided to inform law enforcement of the referenced narratives and theories, which may play in mobilizing criminal actors and DVEs to violence. Generating, accessing, discussing, or otherwise interacting with content related to these theories, without engaging in violence or other criminal activity, is protected by the First Amendment. The FBI does not investigate, collect, or maintain information on U.S. persons solely for the purpose of monitoring First Amendment-protected activities.

² The perception that deaths of like-minded individuals at the hands of law enforcement were unjust has historically been a significant driver for DVEs. DVEs have seized on the deaths of two U.S. persons Vicki and Samuel Weaver at Ruby Ridge, Idaho in 1992; U.S. persons at the Branch Davidians compound at Waco, Texas in 1993; and U.S. person Duncan Lemp in 2020 to justify threats against law enforcement and government officials.



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

DVEs May Target Elected Officials and Government Buildings Following Political Shifts

Perceptions of fraud surrounding the outcome of the General Election and the change in control of the Presidency and Senate—when combined with long-standing DVE drivers such as perceived government or law enforcement overreach, and the anticipation of legislation perceived to oppose or threaten their beliefs— may lead to an increase in the DVE threat.

Narratives surrounding the perceived success of the breach of the U.S. Capitol will likely lead to an increased DVE threat towards federal, state, and local governments across the United States, particularly in the time period surrounding the 20 January Presidential Inauguration. The targeting of government buildings and officials is consistent with observed activity in 2020, when armed individuals, including DVEs, threatened elected officials and occupied state government buildings. Since the 6 January event, online rhetoric regarding the 20 January Presidential Inauguration has increased, with some calling for unspecified “justice” for the 6 January fatal shooting by law enforcement of an individual at the Capitol Building, and another posting that “many” armed individuals would return on 19 January, according to open-source reporting. The recent removal efforts by social media platforms used by DVEs may push some to revert to other platforms they perceive as more secure.

Range of DVE Actors Likely to Pose Increasing Threat at Lawful Protests, Rallies, Demonstrations, etc.

Throughout 2020, DVEs with differing goals and perspectives exploited such events to promote, organize, conspire, and plot against ideological opponents and other targets. DVEs’ efforts to engage in violence at lawful gatherings will probably increase throughout 2021, as some DVEs perceive increased socio-political pressures. Such perceived pressures may stem from, but not be limited to, one or more of the following factors:

- The potential for shifts in various policies many DVEs may perceive to oppose or threaten their ideological goals and agendas or feed into existing narratives many DVEs subscribe to regarding the U.S. government’s exercise of power, influence, and initiatives: possibly including firearm legislation, the easing of immigration restrictions, and new limits on the use of public land.
- Ongoing narratives by DVEs that the 2020 General Election was illegitimate, or fraudulent, and the subsequent belief its results should be contested or unrecognized.
- Some DVEs’ discontent with renewed measures to mitigate the spread of COVID-19, the ordered dissemination of COVID-19 vaccinations, and the efficacy and/or safety of COVID-19 vaccinations.

The FBI, DHS, and NCTC remain concerned about the potential for a loosely organized, sustained, and significant DVE population mobilizing to violence based on social media calls to target government infrastructure or officials. The shared narrative of election fraud and the opposition to the change in control of the executive and legislative branches of the federal government may lead some individuals to adopt the belief that there is no political solution to address their grievances and violent action is necessary. Additionally, in-person engagement between DVEs of differing ideological goals during the Capitol breach likely served to foster connections, which may increase DVEs’ willingness, capability, and motivation to attack and undermine a government they view as illegitimate.³

³ Targeted attacks on identified elected and party officials based upon their political opinions would be similar to attacks observed in the last five years including the 2017 attempted assassination of Republican members of Congress on a baseball field in Virginia, or two assassinations by violent extremists espousing a belief in white supremacy targeting a British member of Parliament, and a German political party official.



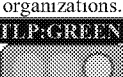



In the near term, DVEs could exploit upcoming events to engage in or justify violence, including events attended by MVEs and “boogaloo”⁴ adherents scheduled nationally from 16 to 20 January; the 20 January Presidential Inauguration and associated events in Washington, D.C.; and the impeachment and possible departure of the 45th President prior to the end of his term. The “boogaloo” is a concept most commonly used to reference an impending second civil war or insurgency against the U.S. Government. Calls for revolution may especially resonate with militia violent extremists (MVEs), who often justify violence based on their belief that they are guardians of the Constitution and the legacies of the American Revolution. While they may not necessarily share the partisan views of those who engaged in the 6 January breach, MVEs and other DVEs who adhere to the “boogaloo” concept and seek a politically motivated civil war, and racially motivated violent extremists who seek a race war, may exploit the aftermath of the Capitol breach in an attempt to create conflict in the United States.

If companies witness any suspicious activities related to potential domestic violent extremism, please report it to your FBI Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.

OPS’s Information Sharing and Analysis Unit disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
 Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

⁴ According to open-source research, the original boogaloo meme references the 1984 film, *Breakin' 2: Electric Boogaloo*. Mainstream culture adopted the phrase “electric boogaloo” to comment on follow-on or repeat events in pop- and political-culture, such as re-elections. MVEs use the boogaloo derivative of the phrase to refer to a second Civil War, i.e. American Civil War 2: Electric Boogaloo. Proponents cultivated the meme by sharing images, videos, and rhetoric. “Big igloo,” “Big luau,” “Boog Bois,” “Boojahideen,” and other associated word-play in addition to imagery such as igloos, Hawaiian shirts, and leis, are used as coded references to the larger boogaloo phenomenon on-and offline.

From: [REDACTED] (FBI) [REDACTED]@fbi.gov]
Sent: 1/15/2021 9:56:49 AM
To: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

If either or both of you have time this morning to discuss SARs and a couple ideas, that would be great.

I will be on my cell this morning.

[REDACTED]

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].
 - Secondly, 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.

From: [REDACTED] (FBI)
Sent: Friday, January 15, 2021 9:56 AM
To: [REDACTED]@bofa.com>; [REDACTED]@bofa.com>
Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

From: [REDACTED]@bofa.com]
Sent: 1/17/2021 7:54:23 PM
To: [REDACTED]@fbi.gov'; [REDACTED]@fbi.gov]
CC: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: RE: [SecMail:] secmail:RE: Follow-up

[REDACTED] – you should have an email from [REDACTED]@bofa.com with our filing on the parameters you discussed with [REDACTED] last week.

Thanks,
[REDACTED]

From: [REDACTED]@fbi.gov [mailto:[REDACTED]@fbi.gov]
Sent: Saturday, January 16, 2021 11:26 AM
To: [REDACTED]@bofa.com>
Cc: [REDACTED]@bofa.com>; [REDACTED]@bofa.com>; [REDACTED]@fbi.gov
Subject: RE: secmail:RE: Follow-up

[REDACTED]

Great. Thanks. I will run with the info.

From: [REDACTED]
Sent: Sat, 16 Jan 2021 15:16:38 +0000
To: [REDACTED] (FBI)
Cc: [REDACTED]
Subject: Follow-up

Hi [REDACTED]

Following up from our conversation yesterday morning, we are doing some work around the parameters we discussed and should have something out before the end of the weekend.

To: [redacted]@keybank.com [redacted]@sc.com [redacted]
[redacted]@sc.com [redacted]@westernunion.com]; [redacted]
[redacted]@westernunion.com [redacted]@wellsfargo.com [redacted]@wellsfargo.com [redacted]@wellsfargo.com [redacted]@paypal.com];
[redacted]@paypal.com [redacted]@paypal.com [redacted]@citi.com]; [redacted]
[redacted]@citi.com [redacted]@bofa.com [redacted]@bofa.com];
[redacted]@santander.us [redacted]@santander.us [redacted]@us.hsbc.com [redacted]
[redacted]@jpmorgan.com [redacted]@us.mufg.jp [redacted]@us.mufg.jp];
[redacted]@wellsfargo.com [redacted]@wellsfargo.com [redacted]@santander.us [redacted]
[redacted]@us.mufg.jp]; [redacted]@citi.com [redacted]@us.hsbc.com];
[redacted]@bofa.com]; [redacted]@bofa.com]

Cc: [redacted]@fincen.gov]; [redacted]@fincen.gov]; [redacted]
[redacted]@fincen.gov]

From: [redacted]@fincen.gov]
Sent: Fri 1/15/2021 4:00:25 PM (UTC-05:00)
Subject: Compiled typologies in advance of 4:30 call
[Jan 15 2021 compiled typologies.docx](#)
[KeyBank Query Logic for Active Shooters v 01-15-2021.pptx](#)

All, in advance of the 4:30 call, please find attached indicators shared by two institutions, as well as indicators developed from prior FinCEN analysis on lone actors/homegrown violent extremists.

Talk to you shortly,
[redacted]

1) Bank submission:

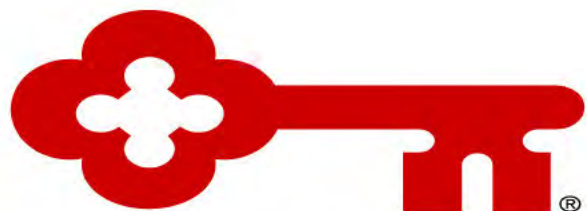
One of the things we've done is search Zelle payment messages for indications of involvement in the riots or potential violence. Here are the key words we used below to pull the data. [...] from our initial analysis "Storm the", "Capitol", "white power" and "Antifa" seem to be yielding the best results.

%PRESIDENT%
%PREZ%
%TRUMP%
%KAMALA%
%BIDEN%
%DIE%
%KILL%
%SHOOT%
%BLOW%
%GUN%
%DEATH%
%MURDER%
KRAKEN
ANTIFA
LAST SONS
OATH KEEPER
WHITE POWER
CAPITOL
STORM THE
CIVIL WAR
GROYPER ARMY
CAMP AUSCHWITZ
AMERICA FIRST
THREEPERS
MILITIA
CAPITAL
MAGA
PATRIOT
BOOGALOO
PROUD B%
CIVIL WAR
PELOSI
PENCE
Schumer

2) Lone Actor/Homegrown Violent Extremism Indicators (developed from prior FinCEN analysis)

- ✓ Long periods of account inactivity, or show normal usage, but in the months or years preceding an attack, a sudden surge or change in activity type.
- ✓ Sudden purchase of firearms, firearm parts and accessories, ammunition, tactical gear at outdoor supply stores, and purchases at shooting ranges not commensurate with previously known customer behavior.

- ✓ Frequent cash deposits of unknown origin, followed by debit or credit card purchases at retailers not commensurate with previously known customer purchase activity.
- ✓ Frequent ATM withdrawals and wire transfers with no apparent economic or business purpose.
- ✓ Sudden account closings, asset liquidations, and disbursements in days or weeks leading up to attacks.
- ✓ Life insurance policy purchases not commensurate with typical behavior for the type of account holder.
- ✓ Transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose or not commensurate with the previous travel history of the customer, for example, travel to high-risk areas or indirect flightpaths for no apparent legitimate reason.
- ✓ Purchases that appear excessive or unusual for hobbyist or other legitimate use.
- ✓ The purchase of pre-cursor chemicals, fireworks, or potential bomb-making equipment, for example, ammonium nitrate, citric acid, aluminum powder, triacetone triperoxide [TATP], potassium nitrate, red iron oxide, tannerite, lengths of piping, BB pellets, cell phones, and others.
- ✓ Purchases of international calling cards not commensurate with previously known customer behavior.
- ✓ The purchase of books (including religious texts) and subscriptions to other media containing extremist views.
- ✓ Donations to organizations known to promote radicalism.



KeyBank's Query Logic for Active Shooters

[REDACTED]
SVP – Compliance Director - Financial Intelligence

[REDACTED]@keybank.com

Active Shooter Detection – Intent of Query

- Intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (“Lone Wolves”).
- Assumes individuals are creatures of habit and tend to frequent and/or shop at the same places when buying the same or similar items, rather than purchasing the same thing at multiple merchants or vendors.
 - Looks for purchases at multiple merchants or vendors who sell weapons and/or ammunition over a shorter period of time.
- Looks for “bursts” of potential suspicious purchase activity, especially when activity not seen previously.
 - Run query periodically, using a rolling lookback period of 60 days.
- Focuses on credit / debit card transaction activity with merchant / vendor counterparties.
 - Looks at specific counterparty Merchant Category Classification Codes (MCC Codes) and distinct merchant IDs.
 - MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID.
 - No minimum dollar threshold for individual transactions.
 - Uses an iterative feedback loop process to build out and refine the exclusion and inclusion keyword lists (detailed in the next slides).
 - Limitations – Due to a lack of industry identifiers for counterparties for other transaction types, does not look at cash, check, ACH, or wire transactions at this time.
- SARs filed for public safety / law enforcement awareness purposes.
- **Alert Example – John Doe makes 5 credit card purchases at 4 different gun shops, plus makes 4 charges at 3 gun ranges, spending \$3,000 on weapons-related transactions over a 5 week period. Doe does not appear to have any previous firearms purchases.**



Active Shooter Detection – Methodology 1 – Keyword EXCLUSION (Broad Focus)

- **Transaction Population:** Query for credit / debit card purchases involving any of the following MCC codes:

- **3484:** Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
- **3489:** Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
- **5091:** Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - * Not universally recognized MCC code
- **5099:** Durable Goods, Not Elsewhere Classified
- **5933:** Pawn Shops
- **5941:** Sporting Goods Stores (largest sellers of firearms and ammunition)
- **5999:** Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
- **7999:** Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)

- **Keyword EXCLUSION (Above transactions must EXCLUDE these keywords / Not exhaustive list):**

- | | | | | | |
|---------------|-----------------|-----------------|--|------------------------|--------------------|
| ▪ Amazon | ▪ Bowling | ▪ Fitness | ▪ Laundry | ▪ Rod | ▪ Tobacco |
| ▪ Angler | ▪ Canoe | ▪ Food | ▪ LifeVantage | ▪ Scuba | ▪ Tools |
| ▪ Archery | ▪ Card | ▪ Football | ▪ Linen | ▪ Shoe | ▪ Vape |
| ▪ Bait | ▪ Carquest | ▪ Gift Shop | ▪ Lodge | ▪ Skate | ▪ Vapor |
| ▪ Baseball | ▪ Cig | ▪ Golf | ▪ Lowe's | ▪ Ski | ▪ Victoriasecret |
| ▪ Bath & Body | ▪ Coffee | ▪ Google | ▪ Mercari (exact) | ▪ Smoke | ▪ Vitamin |
| ▪ Beauty | ▪ Comic | ▪ Graze | ▪ Mktplace | ▪ Snorkel | ▪ Volleyball |
| ▪ Bicycle | ▪ Communication | ▪ Harris Teller | ▪ Music | ▪ Soccer | ▪ Water |
| ▪ Bike | ▪ Danbury Mint | ▪ Hockey | ▪ Party | ▪ Spirit Manufacturing | ▪ Wish.com (exact) |
| ▪ Billy Beez | ▪ DirecTV | ▪ Home Depot | ▪ PayPal (unless it also includes "Gun") | ▪ Square (exact) | ▪ Yoga |
| ▪ Bingo | ▪ Dive | ▪ Hoops | ▪ Pizza | ▪ Storage | ▪ Zoo |
| ▪ Boat | ▪ Ebay | ▪ Hospital | ▪ Pool | ▪ Swim | ▪ Zulily (exact) |
| ▪ Body | ▪ Engineering | ▪ Indeed | ▪ Print | ▪ Tackle | |
| ▪ Body-Solid | ▪ Escrow.com | ▪ iTunes | ▪ Quiver | ▪ Tan | |
| ▪ Boutique | ▪ Farm | ▪ Jewel | ▪ Resort | ▪ Tea | |
| ▪ Bow | ▪ Fish | ▪ Johnson Hlth | | ▪ Tennis | |

- **During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**

- Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, AND
- Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, AND
- Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, AND
- Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.



Active Shooter Detection – Methodology 2 – Keyword INCLUSION (Narrow Focus)

Transaction Population: Query for credit / debit card purchases involving any of the following MCC codes:

- 3484: Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - 3489: Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - 5091: Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - 5099: Durable Goods, Not Elsewhere Classified
 - 5933: Pawn Shops
 - 5941: Sporting Goods Stores (largest sellers of firearms and ammunition)
 - 5999: Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - 7999: Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)
- * Not universally recognized MCC code

Keyword INCLUSION (Above transactions must INCLUDE one of these keywords / Not exhaustive list):

- | | | | | | |
|------------------------|-------------------------------|----------------------|---------------------------|---------------------------|----------------------|
| Academy.com | Cabela's | Edge-Works | HarrisBipods.com | NorthShoreFirearms.com | SOG International |
| Aero Precision | CaLegalMags.com | Manufacturing | ImpactGuns.com | Noveske.com | SouthernOhioGun.com |
| AimSurplus | CarrierComp.com | EKnife Supply | JP Enterprises | NTCTrading.net | SpikesTactical.com |
| AnarchyOutdoors.com | ChattanoogaShooting.com | EKnifeWorks.com | JPRifles.com | Numrich Gun Parts | SportsmansGuide.com |
| Anderson Manufacturing | CheaperThanDirt.com | EliteDefense.com | JSESurplus.com | OpticsPlanet.com | STIGuns.com |
| AR-15.co | ClassicCollectionFirearms.com | FreedomMunitions.com | KAKIndustry.com | OregonRifleworks.com | STI International |
| AR15.com | Gander Mountain | Gander Mountain | Karambit.com | ParkerMountainMachine.com | Taccom |
| B & T Industries | Geissele.com | Geissele.com | KingsFirearmsAndMore.com | RobertsonTradingPost.com | Taccom3G.com |
| backcountry world | CopesDistributing.com | GhostGuns.com | KingsFirearmsOnline.com | Ruger | TaccomCanada.com |
| Bass Pro Shop | DawsonPrecision.com | GhostRunner.com | MidwayUSA.com | SarcoInc.com | TargetSportUSA.com |
| Blade HQ | DeltaDefense.com | Glock | MGMTargets.com | ShootingTargets7.com | WC Wolff Co. |
| BladeOps.com | DeltaTeamTactical.com | Govx.com | Mike Gibson Manufacturing | SIG Sauer | WideOpenSpaces.com |
| BladePlay | Dick's Sporting Goods | GPKnives.com | MikesGunShop.net | SilencerShop.com | WinthropHolsters.com |
| Botach.com | DillonPrecision.com | GrabAGun.com | Mike's Gun and Pawn | Silent Precision | WittMachine.net |
| Boyd'sGunstocks.com | DLTTrading.com | Grindworx.com | MileHighShooting.com | SMKW.com | |
| BravoCompanyUSA.com | DSG (Dick's Sporting Goods) | GunBroker.com | NewFrontierArmory.com | SniperCentral.com | |
| Brownells | Dunkelbergers.com | GunPartsCorp.com | | | |
| Browning | E-SarcoInc.com | GunSprings.com | | | |

During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):

- Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, AND
- Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, AND
- Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, AND
- Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.



Active Shooter Detection – Additional Red Flags to Consider

When Investigators are reviewing financial accounts, besides alerted transactions, other factors Investigators may wish to consider:

- Is the alerted transaction activity consistent with previous activity, or has it begun recently?
- Unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction?
- Any recent purchases of counter-surveillance equipment?
- Any recent purchases of covert / secure communications equipment?
 - Virtual private networks (VPNs), online gaming, prepaid phones / calling cards, etc. transactions?
- Any recent rental of storage facilities?
- Other excessive transactions, especially if not consistent with previous activity?
 - Hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms, etc.
- Excessive ATM, Prepaid Cards, Person-to-Person (P2P), or Virtual Currency transactions?
- Any recent life insurance purchases and/or bank account closures?
- Any life stressor indicators?
 - Recent excessive legal / medical expenses (legal / family status or health challenges)?
 - No payroll deposits? Unemployed? Recently fired or laid off?
 - Delinquent / excessive debt?
- Any social media posts of concern?



Typologies for review as they relate to the events of 1/6/20

Scope: Transactions pulled from 11/3 – 1/12: ATM, CREDIT, DEBIT, with expanded reviews where needed.

#	Typology
1	MCC Codes that, when taken together, demonstrate travel: ex. hotel, rental car, & gas, AND Mileage increasingly further from cardholder's home
2	Cardholder purchases at gun-ammo, sporting goods stores, etc., that demonstrate increases in volume, value, or velocity above average and/or a high % relative to cardholder's available credit.
3	Transactions that contain keyword list matches: a) potential target events, locations, or individuals b) names: i: of those arrested at demonstrations / riots ii: of key leadership in organizations c) code terms and calls to action d) precursor elements to IEDs and firearms
4	Transactions in or near capitols or state capitols at/around 1/6
5	Multiple cards used by one person, for the purchasing of fire arms/ammo etc.
6	Use of business cards (not held by tactical or security firms) for the purchase of arms / ammo
9	Transfers to GiveSendGo or other crowdsourcing sites
10	Purchasing of gift cards; Use of debit cards for Crypto
11	Over/under invoicing for merchant codes at gun clubs with other vendor services (i.e., large transactions for an individual at a snack bar)



NOTE: DIA plans on looking at these typologies holistically, that is no single hit may warrant escalation but more than one could.

DIA plans on, where possible, pulling transaction details for Credit, ATM, and DEBIT card activity.

DIA will look to sort for these typologies via in person vs. online purchases

The condition and contents of data may dictate that DIA will have to alter these typologies, abandon these typologies, and / or adopt new typologies

[REDACTED]@jpmorgan.com>; [REDACTED]@jpmchase.com' <[REDACTED]@jpmchase.com>
Cc: [REDACTED] [SES] <[REDACTED]@fincen.gov>; [REDACTED] <[REDACTED]@fincen.gov>; [REDACTED]
<[REDACTED]@fincen.gov>
Subject: RE: Capitol Riots

All, Key Bank circulated this very helpful list of key terms.

Regards,
[REDACTED]

From: [REDACTED]
Sent: Saturday, January 16, 2021 4:11 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: [REDACTED] [SES] <[REDACTED]@fincen.gov>; [REDACTED] <[REDACTED]@fincen.gov>; [REDACTED]
<[REDACTED]@fincen.gov>
Subject: Capitol Riots

All,

In advance of today's discussion, we have attached a slide from FinCEN containing some key terms applicable to matters related to racially and ethnically motivated violent extremism (REMVE), which may have application to the capitol riots and related activity. Similarly, many additional relevant terms may be found on the Anti-Defamation League website at the following link: <https://www.adl.org/hate-symbols>

MUFG kindly circulated a publicly-available overview on the funding of American hate groups. It can be found at the following link: <https://www.isdglobal.org/wp-content/uploads/2020/10/bankrolling-bigotry-3.pdf>

Additionally, while we know all of you are reviewing public domain information, below are links to a few media reports that are of particular note and may be helpful:

<https://blog.chainalysis.com/reports/capitol-riot-bitcoin-donation-alt-right-domestic-extremism>

<https://www.reuters.com/article/us-usa-election-cryptocurrency/large-bitcoin-payment-made-to-far-right-individuals-before-u-s-capitol-attack-report-idUSKBN29J2PM>

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.mfg.jp [REDACTED]@us.mfg.jp; [REDACTED]@us.mfg.jp [REDACTED]@us.mfg.jp; [REDACTED]@us.mfg.jp [REDACTED]@us.mfg.jp];
[REDACTED]@us.mfg.jp [REDACTED]@us.mfg.jp; [REDACTED]@us.mfg.jp [REDACTED]@us.mfg.jp; [REDACTED]@us.mfg.jp [REDACTED]@us.mfg.jp];
[REDACTED]@unionbank.com [REDACTED]@unionbank.com; [REDACTED]@unionbank.com [REDACTED]@unionbank.com];
[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: [REDACTED] (SES) [REDACTED]@fincen.gov [REDACTED]@fincen.gov; [REDACTED]@fincen.gov; [REDACTED]@fincen.gov];
From: [REDACTED]@fincen.gov [REDACTED]@fincen.gov
Sent on behalf of: [REDACTED]@fincen.gov [REDACTED]@fincen.gov
Sent: Mon 1/18/2021 4:03:27 PM Eastern Standard Time
Subject: RE: Capitol Riots

All, please see below for a potential list of crowdfunding sites we are aware of (including some helpful information for identifying the first two).

[Eventbright.com](#) – People have been observed using this site to post an event and sell tickets including bus tickets to the demonstrations. You may see a Card Purchase with the transaction reference “EB [the EVENT] with the phone number 8014137200.

- For example: EB MARCH FOR TR 801413720 Query by the phone number.

[Aneidot.com](#) – You may see a Card Purchase with the transaction reference in the following format: “A” [a Message or [like a cause or candidate] with the phone number in the following format: 225-2501301.

- For example: A *SMITH 225-2501301 /DC US or A * PAC 225-2501301 /DC US. Query by the phone number.

- Gofundme
- Patreon
- Indiegogo
- RocketHub
- Fundable
- Fundly
- Crowdrise
- Wefunder
- CircleUp
- Fundrazr
- Pozible
- Start some good
- Kiva
- Angel list
- Causes
- Piggybackr
- Youcaring
- Ulule
- Classy
- Realcrowd
- Hatreon
- MakerSupport
- WeSearchr
- GoyFundMe (likely now defunct)
- Rootbocks (likely now defunct)

Regards,

From: [REDACTED]
Sent: Sunday, January 17, 2021 4:06 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]@bofa.com <[REDACTED]@bofa.com>; [REDACTED]@santander.us <[REDACTED]@santander.us>; [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]@wellsfargo.com <[REDACTED]@wellsfargo.com>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@unionbank.com <[REDACTED]@unionbank.com>; [REDACTED]@unionbank.com <[REDACTED]@unionbank.com>; [REDACTED]@unionbank.com <[REDACTED]@unionbank.com>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@us.mfg.jp <[REDACTED]@us.mfg.jp>; [REDACTED]@sc.com <[REDACTED]@sc.com>; [REDACTED]@sc.com <[REDACTED]@sc.com>; [REDACTED]@sc.com <[REDACTED]@sc.com>; [REDACTED]@sc.com <[REDACTED]@sc.com>; [REDACTED]@citi.com <[REDACTED]@citi.com>;