MERCATUS CENTER
George Mason University

STATEMENT FOR THE RECORD

FINANCIAL PRIVACY: LIMITS, DEVELOPMENTS, AND IDEAS FOR REFORM

BRIAN KNIGHT
Director of Innovation and Governance and Senior Research Fellow, Mercatus Center at George Mason University

US Congress, House Financial Services Committee
Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligence (TFI)

February 12, 2024

Thank you, Chairman McHenry and Ranking Member Waters, for the opportunity to submit this statement. My name is Brian Knight, and I am a senior research fellow at the Mercatus Center at George Mason University. My research is on financial services and financial services regulation as a tool of broader regulation, and I also study financial privacy. This statement is intended to help inform the committee of certain issues relevant to its jurisdiction and is not intended to support or oppose any given piece of legislation.

Americans' financial records contain some of the most personally sensitive information available. Yet, under current Supreme Court jurisprudence, Americans lack constitutional privacy protections. Through people's financial records, you could trace—with strong, though not perfect, accuracy—their movements, relationships, health, religion, political views, and activities.

As the Cato Institute's Nicholas Anthony points out,[1] threats to financial privacy have become increasingly ubiquitous as more and more Americans embrace electronic services such as credit and debit cards, automatic deposit, and apps like PayPal, leading to more data collection by financial services providers. This, in turn, has led these same providers to create data types, such as Merchant Category Codes (MCC), on top of consumer-provided information to help manage these transactions. As a collective result, people are being forced to leave a more and more detailed trail of their lives as a condition of engaging with the modern economy.

The very sensitivity and completeness of this data has made it attractive to law enforcement officials and others who hope to use it to surveil, interdict, and prosecute criminals. While these motives are laudable, the United States has long recognized that assisting law enforcement does not grant an

[1] Nicholas Anthony, "The Right to Financial Privacy" (Policy Analysis No. 945, Cato Institute, Washington, DC, May 2, 2023).

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

unlimited justification to use sensitive data, and that precedence must be given to the right of its citizens to meaningful protection from "arbitrary invasions" of their privacy.[2] Additionally, for reasons discussed below, our current financial system may be sacrificing far too much privacy for limited benefit, making itself subject to abuse as a law enforcement tool intending to accomplish by financial regulation what cannot be accomplished by other means.

The remainder of this statement presents the following:

1. A sketch of the limits of financial privacy enjoyed by Americans
2. An overview of recent distressing developments regarding the use of financial records as tools of broad surveillance, including the use of personal data directly related to core constitutional rights
3. Ideas for reform that may inform Congress as it wrestles with how to allow legitimate law enforcement activity while protecting American citizens' privacy in a rapidly evolving world
4. Conclusion

1. LACK OF SUFFICIENT PROTECTION OF CUSTOMER PRIVACY

It is a bitter irony that federal law simultaneously prizes and denigrates the financial privacy of Americans. While laws such as the Gramm–Leach–Bliley Act impose significant duties on financial firms to protect customers' sensitive data from being compromised by outsiders,[3] laws such as the Bank Secrecy Act (BSA) not only enable but often require financial firms to share data with law enforcement without meaningful recourse by the customer.[4] It is as if government is telling customers, "your financial data should be safe and private, except from us." The problem is evident in reporting thresholds and requirements, the emergence of the "third-party doctrine," and informal pressuring by the government.

THE EROSION OF REPORTING THRESHOLDS AND THE EXTENSION OF REPORTING REQUIREMENTS

The problem of privacy infringements has exacerbated over time, as the scope of the BSA has expanded and as inflation has eroded the thresholds that initially limited reporting to relatively large sums. For example, when in 1974 the Supreme Court originally ruled in *California Bankers Association v. Shultz* that the BSA did not violate the Constitution, Justices Powell and Blackmun, who were the margin of victory, noted in their concurrence that because the Department of the Treasury had imposed a $10,000 threshold for reporting, the BSA did not impose an impermissible infringement on privacy.[5] While that threshold for reporting has not changed, the value of the dollar has. The worth of $10,000 in 1974 is approximately $63,900 today.[6] Further, the threshold for mandatory suspicious-activity reporting by banks is currently only $5,000 in aggregate.[7]

[2] See Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[3] Gramm–Leach–Bliley Act, 15 U.S.C. §6801 *et seq.*

[4] Bank Secrecy Act, 12 U.S.C. §1829b; 12 U.S.C §1951–1960; 31 U.S.C §5311 *et seq.*

[5] California Bankers Association v. Shultz, 94 S. Ct. 1494, 1525–1526 (1974).

[6] US Bureau of Labor Statistics, CPI Inflation Calculator (database), accessed February 8, 2024, (https://www.bls.gov/data/inflation_calculator.htm).

[7] 31 C.F.R. §1020.320.

The justices also noted, however, that "a significant extension of the regulations' reporting requirements. . . would pose substantial and difficult constitutional questions."[8] Since 1974 there has been a significant extension of reporting requirements. Today, banks are permitted to voluntarily make reports on any "possible violation of law or regulation" and enjoy protection from liability.[9]

THE EMERGENCE OF "THIRD-PARTY DOCTRINE"

Consumer privacy has been further undercut by the emergence of the "third-party doctrine." For example, in *United States v. Miller*, the Supreme Court found that bank customers lack a privacy interest in their bank records.[10] In the case of checks and similar instruments, the Court reasoned that the customer shared those documents with recipients and banks, and therefore lacked a privacy interest. In the case of the banks' own records, the Court found that those records belonged to the bank, not the customer; therefore, the customer could not have a privacy interest in them.

Even laws to restrain the sharing of information and provide customers with recourse to protect their privacy, such as the Right to Financial Privacy Act (RFPA), provide, at best, extremely limited protection.[11] The RFPA contains so many exceptions to its provisions,[12] including for the reporting of "suspicious activities" under the BSA,[13] as to be almost meaningless. As such, extremely intimate details of a person's life are readily available to the government without substantial due process.

It is worth noting that the Supreme Court has recently refused to expand the logic of *Miller* to cell phone location data.[14] The Court reasoned that the reality of modern life and technology means that people inevitably leave a record of their movements by carrying their phone.[15] The Court also found that allowing the government unfettered access to that data would amount to "near perfect surveillance, as if it had attached an ankle monitor to the phone's user" as well as information about the user's past movements in a way traditional observation does not.[16] The Court also distinguished *Miller* on the grounds that, unlike checks, cell phone data isn't so much shared by the user as much as created automatically.[17]

To be clear, the Court did not overrule *Miller* but rather distinguished it. But when one considers the scope of information that law enforcement can access through modern financial records, the records' retrospective nature, and the need for people to interface with modern forms of financial services to survive, it is not hard to think that *Shultz* and *Miller* have become outdated.

---

[8] *Shultz*, 94 S. Ct. at 1526.

[9] 31 U.S.C. §5318(g); 31 C.F.R. §1020.320(f); see also 12 U.S.C. §3403(c).

[10] United States v. Miller, 96 S. Ct. 1619 (1976).

[11] 12 U.S.C. §3401 *et seq.*

[12] 12 U.S.C. §3413.

[13] 12 U.S.C. §3413(d).

[14] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[15] *Carpenter*, 138 S. Ct. at 2218.

[16] *Carpenter*, 138 S. Ct. at 2219–2220.

[17] *Carpenter*, 138 S. Ct. at 2220.

OPACITY AND GOVERNMENT PRESSURE

In addition to the formal, black-letter law obligations of financial firms under the BSA, there is also the possibility of informal pressure by the government on financial firms to share more information than may be required. Financial services firms are strongly incentivized to file suspicious activity reports (SARs) defensively, even if there is little reason to file them. This is because failure to file a SAR could result in being penalized, whereas excessive filing has no penalty beyond the burden of filing.

Financial services firms, especially banks, are also strongly incentivized to not push back on government requests. Because banks rely on their regulators' good graces to function, and are subject to regular and potentially burdensome supervision as well as a regulatory regime in which perfect compliance is impossible, they are uniquely vulnerable to being punished through informal means.[18] As such, while firms may voluntarily, perhaps even enthusiastically, share data, they may also do so to avoid both formal and informal government sanction.

It is important to recognize how limited the data available to the public and Congress is, regarding the use of SARs and other information sharing. The BSA prohibits notifying a customer if they become the target of a SAR.[19] Moreover, federal and state open records laws do not apply to such reports.[20] While FinCEN will periodically release some information about SARs,[21] it is by no means comprehensive, and it fails to provide insight into how many SARs actually result in meaningful leads or prove essential to preventing serious crimes. This opacity makes it impossible for Congress and the public to meaningfully assess whether the benefits of the system outweigh its burdens, or even what the benefits and burdens actually are.

2. ALLEGATIONS INVOLVING THE USE OF FINANCIAL RECORDS FOR SURVEILLANCE

Recent efforts to explicitly use financial records as a tool of surveillance and mass data collection raise troubling implications for Americans' privacy. These efforts have emerged from both the government and private sector, and while these efforts are at least purported to serve a worthy cause, they also risk producing significant damage for only limited benefit.

The most high-profile use of financial services records are the allegations raised by the House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government. The subcommittee alleged that the FBI worked with banks to obtain records based on broad criteria, such as whether the customer had purchased a firearm and been in Washington, DC, around the January 6 riots.[22] Evidence presented by the subcommittee indicates that law enforcement collaborated with

[18] For a more detailed discussion of this dynamic, please see Julie Hill, "Regulating Bank Reputation Risk," *Georgia Law Review* 54, No. 523 (2020). See also Nicholas R. Parrillo, "Federal Agency Guidance and the Power to Bind: An Empirical Study of Agencies and Industries," *Yale Journal on Regulation*, No. 165 (2019); The Financial and Business Law Scholars as Amici Curiae, 3–27, The National Rifle Association of America v. Maria T. Vullo.

[19] See e.g. 31 U.S.C. §5318(g)(2); 31 C.F.R. §1020(e).

[20] 31 U.S.C §5319.

[21] See e.g. Financial Crimes Enforcement Network, *FinCEN FY 2022 Year in Review*, April 21, 2022.

[22] See US House of Representatives, *Interim Staff Report, Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government*, May 18, 2023; Chairman Jim Jordan, letter to Christopher Wray, Director, Federal Bureau of Investigation (Wray letter), January 17, 2024; Chairman Jim Jordan, House Committee on the Judiciary, letter to Noah Bishoff, AML Officer, Plaid Inc., (Bishoff letter), January 17, 2024.

banks on shaping data requests and used criteria that was both broad and tied directly to constitutionally protected activity, such as the purchase of firearms and religious and political activity.

As a threshold matter, it is important to note that there is limited information publicly available regarding the subcommittee's recent allegations that the FBI, FinCEN, and financial services firms collaborated to obtain large amounts of customer information based on broad and sensitive criteria. As more information is released, the picture may change significantly. Based on what is now available, however, the implications are troubling.

One of the subcommittee's allegations is that Bank of America (BoA) provided, either at the request of the FBI or on its own initiative,[23] a list of customers who (1) used a BoA card in the Washington, DC, area on the days surrounding January 6, (2) purchased a firearm with the card, and (3) traveled to or rented lodging in the DC area at the relevant time.[24] While a significant number of customer records were allegedly provided, it is also alleged that those records were ultimately removed from FBI systems because they "lacked allegations of federal criminal conduct."[25]

The subcommittee also claims that FinCEN circulated materials to financial services firms that recommended using search terms directly related to political activity, such as "MAGA," the purchase of books—including religious books—or the consumption of media that espoused "extremist views."[26] It is not clear what would constitute an extremist view for these purposes, but the potential use of the financial system to monitor Americans' political activity, speech, and religious pursuits is troubling.

FinCEN also allegedly distributed material created by KeyBank discussing ways to identify potential violent extremists using a combination of MCCs, vendor names, and purchase thresholds.[27] Many of the MCCs and other criteria were inherently and dramatically overinclusive, such as those covering sporting-goods stores, pawn shops, or popular retailers like Dick's Sporting Goods and Bass Pro Shops. Of note, some of the MCCs KeyBank used were attached to arms manufacturing. These MCCs were not established by the International Organization for Standardization (ISO) and are not in use by all banks.[28] While many MCCs are standardized, MCC 3000-3999 are "reserved for private use."[29] Therefore, it is possible that banks have established MCCs that may relate to sensitive and constitutionally protected activities that are not publicly known. This would allow banks and the government to more easily search for economic activity that, while controversial, is constitutionally protected or extremely sensitive.[30]

---

[23] There are discrepancies between witness testimony and documents as to whether the FBI or BoA initiated the data exchange.

[24] Wray letter.

[25] Wray letter.

[26] Bishoff letter.

[27] Bishoff letter.

[28] For a greater discussion of the KeyBank MCCs please see Brian Knight, "(Updated) MCCs and Financial Privacy, Again," *FinRegRag*, January 18, 2024.

[29] Knight, "(Updated) MCCs and Financial Privacy, Again."

[30] This concern is by no means shared only by conservatives. After the Supreme Court ruled that there was no right to an abortion under the US Constitution, many were concerned that their banking records could be used to identify them having an abortion. See e.g. Alejandra Caraballo, "Payment Data Could Become Evidence of Abortion, Now Illegal in Some States," *New York Times*, June 29, 2022.

KeyBank is not the only firm that wished to use MCCs as part of a surveillance program. At the prompting of Amalgamated Bank, the City of New York, and various pension funds, ISO established an MCC for gun stores.[31] The justification was that the MCC allowed banks to potentially detect activity that could indicate an imminent crime, especially a mass shooting, and alert law enforcement via a suspicious activity report.[32]

While the desire to prevent violence is laudable, the use of MCCs for this purpose is unlikely to be effective.[33] The data would be both over- and underinclusive, because it would capture information on merchants rather than purchased items. It would also rely on bank personnel being able to assess what was truly suspicious, which is unlikely. Finally, it would add numerous additional SARs, most of which are unrelated to any crime, to a system that already receives over four million SARs per year.[34] It is not clear how many SARs are followed up on, but a small study by the Bank Policy Institute in 2018 found that a median of 4 percent of SARs resulted in a law enforcement follow-up.[35]

While such preemptive surveillance would be unlikely to provide much benefit, it would be expensive to administer and would subject Americans to even more intrusive surveillance. These concerns prompted several states to prohibit the use of the gun store MCC, though California has recently mandated its use.[36] California explicitly justified its law as using financial services as a surveillance tool to preempt crime.[37]

In summary, there is evidence of ongoing—and increasing—efforts to use financial data as a tool of preemptive and sweeping surveillance. These efforts directly target constitutionally protected activities—an outcome that risks significant threat to Americans' rights. It is critical that Congress have a complete picture of how financial surveillance is being used and ensure it conforms to the American model of constitutional self-governance.

3. AREAS OF POSSIBLE REFORM

Efforts to reform the BSA and other data-sharing laws are long-standing. Much excellent work has already been done, and I commend the committee to consider it. For example, the scholars at the Cato Institute have written extensively about ways to more broadly reform the BSA.[38] I will limit my ideas

[31] See Associated Press, "Visa, Mastercard, AmEx to Start Categorizing Sales from Gun Shops," *NBC News*, September 10, 2022; Leah Collins, "Amalgamated Bank CEO on Why We Can and Should Track Gun Purchases on Cards," *CNBC*, July 13, 2022.

[32] Kate Fitzgerald, "Will New Merchant Code for Gun Sales Turn Issuers into Morality Police?" *American Banker*, September 16, 2022.

[33] For a more detailed discussion of why using MCCs to prevent mass shootings would be unlikely to be effective please see Brian Knight, "More Questions about Credit Card MCCs for Gun Stores," *FinRegRag*, September 22, 2022; Brian Knight, "More Thoughts on the Use of MCCs for Law Enforcement Tracking," *FinRegRag*, January 24, 2024.

[34] *FinCEN FY 2022 Year in Review*.

[35] Bank Policy Institute, *Getting to Effectiveness—Report on US Financial Institutions Devoted to BSA/AML and Sanctions Complications* (Washington, DC, October 29, 2018).

[36] Caitlin Mullen, "States Split Over Gun Merchant Category Code," *Payments Dive*, October 2, 2023.

[37] Mullen, "States Split Over Gun Merchant Category Code."

[38] See e.g. Norbert Michel and Jennifer Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," (Policy Analysis No. 932, Cato Institute, Washington, DC, July 26, 2022); Nicholas Anthony, "The Right to Financial Privacy," (Policy Analysis No. 945, Cato Institute, Washington, DC, May 2, 2023).

primarily to areas mentioned in the recent allegations and the efforts to increase the use of the payments system as a tool of preemptive surveillance.

First, greater transparency is essential. FinCEN and other relevant agencies should be required to report to Congress and the public not only the number of SARs and other reports they receive but also the number of SARs and reports that are (1) followed up by law enforcement, (2) used to open new investigations that result in prosecutions and convictions, and (3) not used. The relevant agencies should also report on the time it takes for SARs to be used by law enforcement. This last point is relevant to how effective SARs could be at preempting a crime rather than simply assisting in a post-crime investigation.

Second, Congress should consider mandating that a customer be notified, after a reasonable period, if they are the target of a SAR. If a compelling reason exists, such as an ongoing criminal investigation, law enforcement could petition a court to delay that notification. Otherwise, citizens should eventually know if and why a report was filed on them. This will help the public and Congress better understand how the current SAR system works and assess whether it is worth the cost.

Third, Congress should obtain from FinCEN, other relevant agencies, and financial institutions a complete and up-to-date list of all MCCs and other criteria used by financial services firms to categorize customer transactions, and how that information is reported to the government. The level of possible intrusiveness of financial surveillance is inherently linked to the granularity of the data available.

Fourth, Congress should investigate the nature of interactions between financial institutions and the government around data sharing. The BSA and RFPA appeared to contemplate a largely arm's-length relationship; however, there are indications that the relationship is far more collaborative. If this is the case, changes to the law may be appropriate.

Fifth, Congress should investigate how relevant government agencies and financial institutions view their powers and limitations under the law. Given the secrecy of information sharing, those whose information has been shared find it almost impossible to challenge the exchange in court. This means that the judiciary may not be able to correct mistaken views of the law that government and industry may have. Congress's assessment of whether the understanding of government and industry conforms with both the law and congressional intent will help inform whether reform is necessary.

Sixth, financial institutions should be granted greater legal protection for pushing back in good faith on government requests they believe to be outside the law, or for failing to file SARs when they deem them unreasonable. This protection would need to shield institutions from regulators' informal efforts to punish them through procedural, as well as formal, actions.

Seventh, Congress should explicitly include a reasonableness requirement for all transfers of information, whether voluntary or—due to a compulsive reporting requirement—obligatory. Law enforcement is limited to reasonable suspicion in other contexts, and it should not be different here. That standard should at a minimum prevent "dragnet-style" mass requests, or transfers based on nothing more than location or constitutionally protected activity. It should also allow for the suppression of evidence obtained or derived from unreasonable transfers in a subsequent trial, as well as a customer's private right to action against the government, the financial institution, or both.

Eighth, Congress may wish to consider prohibiting the use of MCCs or other classifying criteria that directly relate to constitutionally protected activities. The most obvious is the purchase of firearms, but criteria that focus on political, religious, or other core constitutional rights could also endanger privacy. Congress may also wish to expand this restriction beyond constitutional rights to other highly sensitive issues such as health care.

Ninth, Congress should create or enhance a body—either within or outside of the relevant agencies—to investigate privacy issues and advocate for the protection of consumer privacy from excessive intrusion. Inspector generals could be one option, and an independent body could be another.

Finally, Congress should establish a clear statutory right to allow its members and staffers to access relevant data from government agencies. Their access would be subject to proper handling requirements and necessary customer privacy protections, but without the agencies' ability to prevent or unduly impede access. This is essential to meaningful oversight.

4. CONCLUSION

Americans' lives are written in their bank accounts. Engaging with the modern economy necessitates that Americans leave a trail of information that can be used to build a reasonably accurate and complete picture of a person's travels, interests, beliefs, and problems. This information is regarded by the government as extremely sensitive, yet it enjoys severely limited protection from government intrusion.

While sharing information on consumers may, at times, be useful to law enforcement, it also poses serious risks of abuse and excessive intrusion into the private lives of Americans. This country was founded on the notion that the government should not have a general warrant to surveil its citizens, and that even the legitimate needs of law enforcement must be balanced against, and often subsumed by, the need to protect reasonable privacy.

Recent events and allegations raise concerns that this balance is increasingly slighted. Congress should mandate greater transparency, examine the current system, and initiate reforms as appropriate to preserve legitimate law enforcement capabilities within the limits of meaningful privacy protections.