



November 26, 2024

Submitted electronically via Regulations.gov

Matthew G. Olsen  
Assistant Attorney General for National Security  
U.S. Department of Justice, National Security Division  
950 Pennsylvania Avenue NW  
Washington, D.C. 20530

Re: Federal Register No. 2024-24582  
Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and  
Government-Related Data by Countries of Concern or Covered Persons

Dear Assistant Attorney General Olsen:

The Securities Industry and Financial Markets Association (“SIFMA”), Futures Industry Association (“FIA”) and Institute for International Bankers (“IIB”) appreciate the opportunity to comment on the proposed rulemaking concerning bulk data transfers to countries of concern.

### **Commentors**

SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (“GFMA”).

FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C. FIA’s membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from about 50 countries as well as technology vendors, law firms and other professional service providers. FIA’s mission is to support open, transparent and competitive markets; protect and enhance the integrity of the financial system; and promote high standards of professional conduct.

IIB represents the U.S. operations of internationally headquartered financial institutions from more than 35 countries around the world. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer

subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions also enhance the depth and liquidity of U.S. financial markets and contribute significantly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

## **Background and Recommendations**

As you are aware, on February 28, 2024, President Biden announced an Executive Order (“EO”) 14117 directing the Department of Justice (“DOJ”) to promulgate regulations that restrict or prohibit transactions involving certain bulk transfers of sensitive personal data or United States Government-related data to countries of concern or covered persons.<sup>1</sup> As directed by the EO, on March 5, 2024, the DOJ published in the Federal Register an Advance Notice of Proposed Rulemaking (“ANPRM”) regarding “Access to Americans’ Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern.”<sup>2</sup> Following the ANPRM, on October 29, 2024, the DOJ published in the Federal Register a Notice of Proposed Rulemaking (“NPRM”) regarding “Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons.”<sup>3</sup>

Our members conduct thousands of data transfers every hour, completing transactions on behalf of millions of investors around the globe. As such, the DOJ’s final rule will have a significant impact on how our members conduct business and, as a result, how millions of Americans access the financial markets. Therefore, it is critical that the DOJ, in finalizing its rule, use precise language to ensure the financial services industry is not unduly burdened. We respectfully submit that our recommendations below comport with the ANPRM’s aspiration to “carefully calibrate” the enhancement of national security while “minimizing disruption to commercial activity.”<sup>4</sup>

*Excluded Financial Services.* In SIFMA’s ANPRM comments,<sup>5</sup> we requested the DOJ make clear that the financial services exemption covers “data transfers that are ‘ordinarily incident to and part of’ investment advisory relationships, broker-dealer transactions, and securities transfers are included as covered transactions that are ‘ordinarily incident to and part of the

---

<sup>1</sup> Exec. Order No. 14,117, Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (Feb. 28, 2024), *available at* <https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related> [hereinafter EO].

<sup>2</sup> National Security Division; Provisions Regarding Access to Americans’ Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780 (proposed Mar. 5, 2024), *available at* <https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and> [hereinafter ANPRM].

<sup>3</sup> National Security Division; Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 Fed. Reg. 86116 (proposed Oct. 29, 2024), *available at* <https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data> [hereinafter NPRM].

<sup>4</sup> 89 FR 15782.

<sup>5</sup> SIFMA Comment Letter on DOJ ANPRM re Bulk Data Transfers, DOJ-NSD-2024-0002-0030, (Apr. 18, 2024) *available at* <https://www.regulations.gov/comment/DOJ-NSD-2024-0002-0030>.

provision of financial services.”<sup>6</sup> We appreciate the DOJ taking this proposal under consideration and including a specific exemption for investment management services in § 202.505(6) of the NPRM. The inclusion of this exemption will help ensure that the proposed regulations avoid unnecessarily burdening transfers that are otherwise already well-regulated by the various financial services self-regulatory and other regulatory bodies. We recommend the DOJ maintain this exemption in its final rule.

To further clarify, as there are operational and compliance activities ordinarily incident to financial institutions that are not necessarily common to other sectors, and in order to avoid confusion as to whether such activities are separately addressed under the exception for corporate group transactions under § 202.506, we would recommend further including the following clarification in § 202.505(a):

Subparts C and D of this part do not apply to data transactions, to the extent that they are ordinarily incident to and part of the provision of financial services *or the operations of financial services entities* regulated by Financial Industry Regulatory Authority, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation, the National Credit Union Administration, or state banking or insurance regulators, including without limitation:

*Including Regulatory Compliance in the Exemption.* To avoid any uncertainty, it would also be useful to expressly mention that data transfers that facilitate or are related to compliance with regulatory obligations of financial services entities are included within the exemption. This would, for example, include activities pertaining to sanctions compliance, anti-money laundering compliance, “Know Your Customer” rules, FCRA and other data privacy inquiries, securities exchange compliance and other requirements. and response to inquiry by regulatory or self-regulatory authorities. Therefore, we recommend the following be included as an enumerated exemption:

(8) data transfers that facilitate or otherwise relate to the compliance with a financial industry entity’s regulatory obligations and compliance with applicable law.

*Including Futures in the Exemption.* The current express references to securities transactions and the Securities Exchange Act in connection with the financial services, however, may inadvertently suggest that futures and derivatives transactions are not also included within the scope of the exemption. To avoid any uncertainty, we ask that the DOJ expressly clarify that futures, options and derivatives or other transactions subject to the jurisdiction of the Commodity Futures Trading Commission (“CFTC”) under the Commodity Exchange Act are also exempt. Furthermore, the exemption should explicitly cover security-based swaps as well as the activities

---

<sup>6</sup> *Id.* at 3

of Futures Commission Merchants (“FCMs”), commodity trading advisors, introducing brokers and other CFTC-regulated entities, their activities being “ordinarily incident to and part of the provision of financial services” within the meaning of the rule.

*Asset-Backed Securities.* The DOJ’s approach may also be unintentionally harmful to mortgage-backed securities and other asset-backed securities that involve significant personal data in the underlying assets. Securitization of these assets is fundamental to the efficient operation of U.S. financial markets, and it creates more capital for Americans to buy homes. Following the 2008 crisis, it was highly important for purchasers of these securities to be able to access and check (usually on a sampling basis) the robustness of the underlying assets. It is not our understanding that the DOJ wishes to curtail the ability of parties in countries of concern from buying securities backed by U.S. mortgages and other assets, and we recommend that such assets also be expressly exempted to avoid any uncertainty.

*Passive Investment Threshold.* We also appreciate the NPRM’s exclusion of passive investments from the definition of “investment agreement.”<sup>7</sup> We agree with the DOJ’s finding that “passive investments...do not pose an unacceptable risk to national security.”<sup>8</sup> Based on this same rationale, DOJ should be able to be more inclusive of additional passive investments by raising the 10 percent de minimis threshold to 35 percent. Numerous minority investments have more than 10 percent of total voting and equity interest and are still entirely “passive.” Furthermore, the third requirement of the “passive investment” definition should give the DOJ comfort in raising the threshold because once a covered person has “rights beyond those reasonably considered to be standard minority shareholder protections” the investment would no longer be considered passive. Therefore, we encourage DOJ to raise the passive investment threshold.

*Definition of Data Brokerage.* We recommend that the DOJ further clarify the definition of “data brokerage” to exclude any activity that is subject to an exemption under the proposed regulations, for example § 202.505. This clarification is necessary to ensure that the proposed regulations do not inadvertently capture transactions that are already well-regulated by financial services regulators.

*Definition of Bulk.* For financial transactions that do not fall into the above exemptions, we recommend the DOJ change its bulk thresholds for covered data transactions. Specifically, we request the DOJ increase the number of U.S. persons’ personal financial data required to be considered “bulk” and decrease the period under which the proposed regulations calculate the bulk numbers.

We were surprised that in the ANPRM the DOJ assessed that the bulk threshold for personal financial data would fall within 1,000 and 1,000,000, but then decided to pick 10,000 in the NPRM, which is a number much lower than the DOJ’s initial analysis would suggest. Many of our members are large financial institutions that conduct transactions with personal financial data that will easily exceed the current bulk threshold of 10,000. As a result, our members will

---

<sup>7</sup> NPRM, supra note 3, at 86209.

<sup>8</sup> *Id.* at 86133.

have to review every transaction that could potentially be considered “restricted,” which will significantly increase regulatory burdens and costs.<sup>9</sup>

Compounding the problem of the DOJ’s selection of the lower number for the bulk threshold is the 12-month lookback period. As currently written, for a multi-national financial services company that may have thousands of such data flows, “bulk” may be rendered meaningless, because for every transaction that may be covered, no matter how small, our members will have to scrutinize and conduct thorough recordkeeping because it may be compounded with a few more transactions to reach the threshold. If an entity conducts just two transactions a month related to 450 U.S. individuals’ personal financial data over the 12-month period, that would be considered a bulk transaction.

In sum, the lookback period is too long and the bulk threshold too low. The combination of the lookback and the low threshold creates significant burdens to conducting financial activity that, in our view, the Executive Order did not intend. Thus, we recommend the DOJ increase the bulk threshold to 500,000, which is in the middle of what the DOJ previewed in the ANPRM and reflects the realities of entities transferring personal financial data. We further suggest that DOJ eliminate the lookback period so that each transaction can be readily evaluated on its own merits, with a provision that any transaction that was divided for purposes of being under the threshold should be considered as undivided. The elimination of the lookback period is particularly important for practical compliance for large organizations that cannot readily determine all data transactions across multiple lines of business.

*Knowledge.* We recommend the proposed rules limit the definition of “knowingly” to actual knowledge so that the definition would read: “the term ‘knowingly,’ with respect to conduct, a circumstance, or a result, means that a person has actual knowledge of the conduct, the circumstance, or the result.” We think this knowledge standard more aligns with the directed component of the prohibition in § 202.305. We do not think that a U.S. person should be liable for directing a prohibited or restricted transaction without having actual knowledge of that prohibited or restricted transaction, and this standard should apply regardless of whether the U.S. person is employed by a U.S. firm or a non-U.S. firm (other than for countries of concern of course). If the knowledge standard is too broad and vague, our members will have to scrutinize every transaction to see if it might be reported to a U.S. person, thus adding more regulatory costs and burden. We think this change will bring more certainty to transactions with non-covered persons and would not add any additional national security risk.

---

<sup>9</sup> We understand that the DOJ considered seven factors when determining the sensitivity of personal financial data, but based on its analysis, personal financial data is the second least sensitive category. We believe that personal financial data is less sensitive than the current DOJ analysis suggests, and therefore, should not be grouped with personal health data, and thus should have a higher bulk threshold. Changeability and velocity should point towards personal financial data being less sensitive than the current DOJ analysis. For velocity, the DOJ analysis cherry-picks a very specific type of data to make it seem that there is varied velocity, but the vast majority of financial data can only be used for a short time. Additionally, the DOJ underweights the ability of individuals to change their financial identifiers, which is more common than the DOJ analysis suggests. Importantly, as the DOJ already found, personal financial data is less sensitive than personal health data and the two should not be grouped together.

*Timing.* Although the effective date of these regulations is not clear at present, we request that those covered be given at least 12 months to implement responsive changes, as these restrictions may require the reorganization of complex business flows, relocation of resources, and development and testing of new systems. Given the significant modifications that need to be implemented for covered institutions, a shorter implementation timeframe will only cause unnecessary disruption to critical commercial activity, undermining one of the key aspirations of the Executive Order and the NPRM.

\* \* \* \* \*

We appreciate your consideration of this request. If you have questions or would like to discuss these comments further, please reach out to Melissa MacGregor at [mmacgregor@sifma.org](mailto:mmacgregor@sifma.org).

Sincerely,

*Melissa MacGregor*

Melissa MacGregor  
Deputy General Counsel &  
Corporate Secretary  
SIFMA

*Allison Lurton*

Allison Lurton  
General Counsel &  
Chief Legal Officer  
FIA

*Stephanie Webster*

Stephanie Webster  
General Counsel  
IIB