PREVENTING ACCESS TO US SENSITIVE PERSONAL DATA AND GOV'T RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

PERSONAL FINANCIAL DATA

Background

DoJ Perspective on National Security Risk Posed by Financial Data

- "Financial data tied to individuals can pose associated national security threats in the hands of foreign adversaries."
- "There is also an associated threat to national security to U.S. persons who might be targeted for recruitment by a foreign adversary through the use of financial data as leverage over such U.S. persons."
- "Data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities and debts, and transactions; or data in a credit or "consumer report" expose that individual to more than monetary losses."
- "The threat of exposing an individual's spending habits, particularly spending that may be embarrassing, can render that person open to extortion or blackmail. In instances where a threatened individual has access to especially sensitive information, national security may be at risk."

Key Terms - Definitions

- **202.210 – Covered Data Transaction**

(a) *Definition.* A *covered data transaction* is any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data and that involves:

- (1) Data brokerage;
- (2) A vendor agreement;
- (3) An employment agreement; or
- (4) An investment agreement.

- **202.201 – Access**

The term *access* means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software.

202.240: Personal Financial Data

The term ***personal financial data*** means data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities, debts, or trades in a securities portfolio; or data in a credit report or in a "consumer report" (as defined in 15 U.S.C. 1681a(d)).

- **202.205 – Bulk**

The term *bulk* means any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person:

- (e) ***Personal financial data*** … on more than 10,000 U.S. persons; or

- (g) Combined data, meaning any collection or set of data that contains more than one of the categories in paragraphs (a) through (g) of this section, or that contains any listed identifier linked to categories in paragraphs (a) through (e) of this section, where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

- **202.206 – Bulk US sensitive personal data**

The term *bulk U.S. sensitive personal data* means a collection or set of bulk data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

- **202.249 – Sensitive personal data**

Definition. The term *sensitive personal data* means covered personal identifiers, precise geolocation data, biometric identifiers, human genomic data, personal health data, ***personal financial data***, or any combination thereof.

Exclusions. The term *sensitive personal* data excludes:

- (1) Public or nonpublic *data that doesn't relate to an individual*;
- (2) Data that is… lawfully *available to the public* from a Federal, State, or local government record (such as court records) or in widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories);
- (3) *Personal communications*; and
- (4) Information or *informational materials*.

Predicate Acts – Restricted Transactions involving Personal Financial Data

- **202.401 – Restricted Transactions (e.g,. Personal Financial Data)**

- [N]o U.S. person … may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements required by subpart D of this part and all other applicable requirements under this part.

Financial Data Exemptions

202.505 – Financial Services Exemption

Exemption for data transactions that are ordinarily incident to and part of the provision of financial services, including:

- (1) Banking, capital-markets (including investment-management services), or financial-insurance services; (2) A financial activity authorized for national banks by 12 U.S.C. 24 (Seventh) and rules and regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;
- (3) An activity that is "financial in nature or incidental to such financial activity" or "complementary to a financial activity," section (k)(1), as set forth in section (k)(4) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;
- (4) The transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces);
- (5) The provision or processing of payments or funds transfers (such as person-to-person, business-to-person, and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers, or the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration); and
- (6) The provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to investment-management services (such as broker-dealers executing trades within a securities portfolio based upon instructions from an investment advisor).

• 202.505: When Does the Financial Services Exemption Apply?

(1) *Example 1*. A U.S. company engages in a data transaction to transfer personal financial data in bulk to a financial institution that is incorporated in, located in, or subject to the jurisdiction or control of a country of concern to clear and settle electronic payment transactions between U.S. individuals and merchants in a country of concern where both the U.S. individuals and the merchants use the U.S. company's infrastructure, such as an e-commerce platform. Both the U.S. company's transaction transferring bulk personal financial data and the payment transactions by U.S. individuals are exempt transactions.

(2) *Example 2*. As ordinarily incident to and part of securitizing and selling asset-backed obligations (such as mortgage and nonmortgage loans) to a covered person, a U.S. bank provides bulk U.S. sensitive personal data to the covered person. The data transfers are exempt transactions.

(3) *Example 3*. A U.S. bank or other financial institution, as ordinarily incident to and part of facilitating payments to U.S. persons in a country of concern, stores and processes the customers' bulk financial data using a data center operated by a third-party service provider in the country of concern. The use of this third-party service provider is a vendor agreement, but it is an exempt transaction that is ordinarily incident to and part of facilitating payment.

(4) *Example 4*. Same as Example 3, but the underlying payments are between U.S. persons in the United States and do not involve a country of concern. The use of this third-party service provider is a vendor agreement, but it is not an exempt transaction because it is not ordinarily incident to facilitating this type of financial activity.

(5) *Example 5*. As part of operating an online marketplace for the purchase and sale of goods, a U.S. company, as ordinarily incident to and part of U.S. consumers' purchase of goods on that marketplace, transfers bulk contact information, payment information (*e.g.,* credit-card account number, expiration data, and security code), and delivery address to a merchant in a country of concern. The data transfers are exempt transactions because they are ordinarily incident to and part of U.S. consumers' purchase of goods.

(6) *Example 6*. A U.S. investment adviser purchases securities of a company incorporated in a country of concern for the accounts of its clients. The investment adviser engages a broker-dealer located in a country of concern to execute the trade, and, as ordinarily incident to and part of the transaction, transfers to the broker-dealer its clients' covered personal identifiers and financial account numbers in bulk. This provision of data is an exempt transaction because it is ordinarily incident to and part of the provision of investment-management services.

• 202.505: When Does the Financial Services Exemption Apply? (cont'd)

(7) *Example 7*. A U.S. company that provides payment-processing services sells bulk U.S. sensitive personal data to a covered person. This sale is prohibited data brokerage and is not an exempt transaction because it is not ordinarily incident to and part of the payment-processing services provided by the U.S. company.

(8) *Example 8*. A U.S. bank facilitates international funds transfers to foreign persons not related to a country of concern, but through intermediaries or locations subject to the jurisdiction or control of a country of concern. These transfers result in access to bulk financial records by some covered persons to complete the transfers and manage associated risks. Providing this access as part of these transfers is ordinarily incident to the provision of financial services and is exempt.

(9) *Example 9*. A U.S. insurance company underwrites personal insurance to U.S. persons residing in foreign countries in the same region as a country of concern. The insurance company relies on its own business infrastructure and personnel in the country of concern to support its financial activity in the region, which results in access to the bulk sensitive personal data of some U.S.-person customers residing in the region, to covered persons at the insurance company supporting these activities. Providing this access is ordinarily incident to the provision of financial services and is exempt.

(10) *Example 10*. A U.S. bank operates a foreign branch in a country of concern and provides financial services to U.S. persons living within the country of concern. The bank receives a lawful request from the regulator in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch. Responding to the regulator's request, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.

(11) *Example 11*. A U.S. bank voluntarily shares information, including relevant bulk sensitive personal data, with financial institutions organized under the laws of a country of concern for the purposes of, and consistent with industry practices for, fraud identification, combatting money laundering and terrorism financing, and U.S. sanctions compliance. Sharing this data for these purposes is ordinarily incident to the provision of financial services and is exempt.

(12) *Example 12*. A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. In connection with the board's data security and cybersecurity responsibilities, the director could access the bulk personal financial data. The appointment of the director, who is a covered person, is a restricted employment agreement and is not exempt because the board member access to the bulk personal financial data is not ordinarily incident to the U.S. company's provision of wealth-management services.

Financial Services Exemption – Additional Details

- DoJ is considering whether and how the financial-services exemption should apply to employment and vendor agreements between U.S. financial-services firms and covered persons where the underlying financial services provided do not involve a country of concern.
- Under this exemption, U.S. persons would be required to evaluate whether a particular data transaction (such as a transaction involving data brokerage or a vendor, employment, or investment agreement) is "ordinarily incident to and part of" the provision of financial services such that it is treated as an exempt transaction.
- At one end of the spectrum, if a U.S. financial institution or financial-services company uses a data center operated by a covered person in a country of concern to facilitate payments to U.S. persons in that country of concern, the proposed rule would treat that vendor agreement as "ordinarily incident to and part of" the facilitation of those payments—and thus exempt. *See* § 202.505(b)(3).
- On the other end of the spectrum, if a U.S. financial institution or financial-services company hires a covered person as a data scientist with access to its U.S. customers' bulk personal financial data to develop a new app that could be sold as a standalone product to the company's customers, the proposed rule would treat this employment agreement as not "ordinarily incident to and part of" the financial services provided by the U.S. company—and thus not exempt. *See* § 202.217(b)(4).

Financial Services Exemption – Additional Details (2)

- Between those two ends of the spectrum, DoJ is considering whether the transactions in the following new examples should be treated as exempt transactions or as restricted transactions:
- *New example in § 202.505(b)(4)*. Same as Example 3 (*see* § 202.505(b)(3)), but the underlying payments are between U.S. persons in the United States and do not involve a country of concern: A U.S. bank or other financial institution, to facilitate payments that do not involve a covered person or country of concern (*e.g.,* between U.S. persons in the United States), stores and processes the customers' bulk financial data using a data center operated by a third-party service provider in a country of concern, which is a covered person. Should the vendor agreement with the covered person, which is otherwise a restricted transaction, be treated as "ordinarily incident to and part of" the U.S. financial institution's facilitation of payments that do not involve a covered person or country of concern?
- *New example in § 202.505(b)(12)*. A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. In connection with the board's data security and cybersecurity responsibilities, the director could access the bulk personal financial data. Should the employment agreement with the covered person as a board director, which is otherwise a restricted transaction, be treated as "ordinarily incident to and part of" the U.S. company's provision of wealth-management services to its U.S. clients?
- DoJ is tentatively considering treating the transactions in both examples as restricted transactions because it does not believe that an employment agreement (including the hiring of board members) or a vendor agreement that gives a covered person access to U.S. persons' bulk sensitive personal data is a reasonable and typical practice in providing the underlying financial services that do not otherwise involve covered persons or a country of concern. These transactions therefore appear to pose the same unacceptable national security risk regardless of the kinds of underlying services provided by the U.S. person. The Department welcomes public comment to inform its resolution of this issue, including the extent to which it is reasonable, necessary, and typical practice for U.S. financial-services firms to hire covered persons as employees or vendors with access to U.S. persons' bulk sensitive personal data as part of providing financial services that do not involve a country of concern; why U.S. financial-services firms hire covered persons instead of non-covered persons in those circumstances; and any additional compliance costs that would be incurred if the transactions in these examples were treated as restricted transactions. In addition, after issuance of the final rule, the Department intends to consult the Department of the Treasury and Federal financial regulatory agencies as part of issuing any guidance or advisory opinions regarding the application of the financial-services exemption.

Corporate Group Exemptions & Financial Data

• 202.506 – Corporate Group Transactions Exemption

Exemption for data transactions:

(1) Between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and

(2) Ordinarily incident to and part of administrative or ancillary business operations, including:

- (i) Human resources;
- (ii) Payroll, expense monitoring and reimbursement, and other corporate financial activities;
- (iii) Paying business taxes or fees;
- (iv) Obtaining business permits or licenses;
- (v) Sharing data with auditors and law firms for regulatory compliance;
- (vi) Risk management;
- (vii) Business-related travel;
- (viii) Customer support;
- (ix) Employee benefits; and
- (x) Employees' internal and external communications.

• 202.506: When Does the Corporate Group Transaction Exemption Apply to Financial Services?

(1) *Example 1*. A U.S. company has a foreign subsidiary located in a country of concern, and the U.S. company's U.S.-person contractors perform services for the foreign subsidiary. As ordinarily incident to and part of the foreign subsidiary's payments to the U.S.-person contractors for those services, the U.S. company engages in a data transaction that gives the subsidiary access to the U.S.-person contractors' bulk personal financial data and covered personal identifiers. This is an exempt corporate group transaction.

(2) *Example 2*. A U.S. company aggregates bulk personal financial data. The U.S. company has a subsidiary that is a covered person because it is headquartered in a country of concern. The subsidiary is subject to the country of concern's national security laws requiring it to cooperate with and assist the country's intelligence services. The exemption for corporate group transactions would not apply to the U.S. parent's grant of a license to the subsidiary to access the parent's databases containing the bulk personal financial data for the purpose of complying with a request or order by the country of concern under those national security laws to provide access to that data because granting of such a license is not ordinarily incident to and part of administrative or ancillary business operations.

(3) *Example 3*. A U.S. company has a foreign subsidiary located in a country of concern that conducts research and development for the U.S. company. The U.S. company sends bulk personal financial data to the subsidiary for the purpose of developing a financial software tool. The transaction is not an exempt corporate group transaction because it is not ordinarily incident to and part of administrative or ancillary business operations.

(4) *Example 4*. Same as Example , but the U.S. company has a foreign branch located in a country of concern instead of a foreign subsidiary. Because the foreign branch is a U.S. person as part of the U.S. company, the transaction occurs within the same U.S. person and is not subject to the prohibitions or restrictions. If the foreign branch allows employees who are covered persons to access the bulk personal financial data to develop the financial software tool, the foreign branch has engaged in restricted transactions.

GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

Please direct any questions to gdainfo@bsa.org