ALERT MEMORANDUM

DOJ Issues Final Rule Targeting Bulk Sensitive Personal and U.S. Government-Related Data Transactions Involving Countries of Concern

February 17, 2025

On December 27, 2024, the U.S. Department of Justice, National Security Division ("DOJ") issued a final rule implementing a new regulatory program designed to prevent certain countries (China, Cuba, Iran, North Korea, Russia, and Venezuela) and covered persons from having access to Americans' bulk sensitive personal data and U.S. government-related data ("Final Rule").[1] The Final Rule, which implements Executive Order ("E.O.") 14117 issued on February 28, 2024, builds on an Advanced Notice of Proposed Rulemaking published March 5, 2024, which we previously discussed here, and a Notice of Proposed Rulemaking published on October 29, 2024.[2] The Final Rule will enter into effect on April 8, 2025. However, certain due diligence, audit, and reporting requirements will not require compliance until October 6, 2025.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

Chase Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

Sam Chang
+1 202 974 1816
sachang@cgsh.com

B.J. Altvater
+1 202 974 1584
baltvater@cgsh.com

Ryan Brown
+1 202 974 1746
rybrown@cgsh.com

[1] The regulations implementing the Final Rule will be codified at 28 C.F.R. Part 202.
[2] E.O. 14117 expanded the scope of E.O. 13873, which also serves as the basis for the new U.S. Department of Commerce, Bureau of Industry and Security ("BIS") information and communications technology and services ("ICTS") regulatory program, which we previously discussed here.

As discussed in further detail below, the Final Rule prohibits or restricts U.S. persons[3] from engaging in so-called "covered data transactions,"[4] which include transactions that involve any access[5] by a country of concern or covered person to any bulk U.S. sensitive personal data or government-related data and that involve: (i) data brokerage; (ii) a vendor agreement; (iii) an employment agreement; or (iv) an investment agreement. As discussed below, the Final Rule includes exemptions for certain transactions that otherwise would be considered covered data transactions.

Unlike the Health Insurance Portability and Accountability Act ("HIPAA"), which restricts the sale of certain personal health information without patient consent, the Final Rule contains no consent exemption and is broader in scope. Additionally, unlike the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA"), which require granting consumers the right to opt out of sales of their personal data, the Final Rule does not contain an individual opt-out mechanism, instead focusing on transactions that could grant foreign adversaries access to large quantities of sensitive data.

Introduction to Key Concepts

Under the Final Rule, countries of concern, covered persons, bulk U.S. sensitive personal data, and government-related data are critical concepts. With that in mind, before exploring the types of transactions covered by the regime, we highlight these key concepts below.

Countries of Concern and Covered Persons

The following countries are designated as countries of concern under the Final Rule:[6]

— China, including Hong Kong and Macau;

— Cuba;

— Iran;

— North Korea;

— Russia; and

— Venezuela.

"Covered persons" include:[7] (1) a foreign entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or other covered persons; or that is organized or chartered under the laws of, or has its

[3] U.S. persons include any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. § 1157 or granted asylum under 8 U.S.C. § 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

[4] "Transaction" means any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property (broadly defined to include tangible, intangible, and contingent interests) in which a foreign country or national thereof has an interest. "Transfer" means any actual or purported act or transaction, whether or not evidenced by writing, and whether or not done or performed within the United States, the purpose, intent, or effect of which is to create, surrender, release, convey, transfer, or alter, directly or indirectly, any right, remedy, power, privilege, or interest with respect to any property.

[5] "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.

[6] "Country of concern" means a foreign government that has engaged in a long-term pattern or serious instances of conduct significantly adverse to U.S. national security or security and safety of U.S. persons and that poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of U.S. national security or security and safety of U.S. persons. Countries of concern may be designated by the Attorney General in consultation with the Secretary of State and Secretary of Commerce.

[7] Such covered persons are those that the Attorney General determines to (i) be or may become owned or controlled by, or subject to the jurisdiction or direction of, a country of concern or covered person; (ii) act, have acted, or purported to act, or is likely to act for or on behalf of a country of concern or covered person; or (iii) have knowingly caused or directed, or is likely to knowingly cause or direct, a violation of the Final Rule. Names of people designated as covered persons will be published in a list in the Federal Register and on the DOJ website.

principal place of business in, a country of concern; (2) a foreign individual who is an employee or contractor of a country of concern or a covered person; and (3) a foreign individual who is primarily resident in a country of concern. In addition, the Attorney General, after consultation with the U.S. Department of State, may designate additional covered persons based on certain criteria.

Bulk U.S. Sensitive Personal Data and Government-Related Data

"Sensitive personal data" means covered personal identifiers,[8] precise geolocation data,[9] biometric identifiers,[10] human 'omic data,[11] personal health data,[12] personal financial data,[13] or any combination thereof.[14] "Bulk U.S. sensitive personal data" means a collection or set of sensitive personal data relating to

[8] "Listed identifier" means any piece of data including government IDs, financial account numbers, device identifiers, demographic or contact information, advertising IDs, account-authentication data, network identifiers, or call-detail data. A "covered personal identifier" means any of those listed identifiers: (1) in combination with any other listed identifier; or (2) in combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data. The term covered personal identifiers excludes:

> (1) Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and (2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.

[9] "Precise geolocation data" means data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters.

[10] "Biometric identifiers" means measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.

[11] Human 'omic data is a catch-all term that includes human genomic data, human epigenomic data, human proteomic data, and human transcriptomic data as follows:

- Human genomic data: Data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. § 300gg-91(d)(17)) and any related human genetic sequencing data.
- Human epigenomic data: Data derived from a systems-level analysis of human epigenetic modifications, which are changes in gene expression that do not involve alterations to the DNA sequence itself. These epigenetic modifications include modifications such as DNA methylation, histone modifications, and non-coding RNA regulation.
- Human proteomic data: Data derived from a systems-level analysis of proteins expressed by a human genome, cell, tissue, or organism.
- Human transcriptomic data: Data derived from a systems-level analysis of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. However, the term human 'omic data excludes pathogen-specific data embedded in human 'omic data sets.

[12] "Personal health data" means health information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.

[13] "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)).

[14] Sensitive personal data, and each of the categories of sensitive personal data, excludes:

> (1) Public or nonpublic data that does not relate to an individual, including such data that meets the

U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds certain applicable thresholds.[15]

"Government-related data" means any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List contained in the Final Rule that the Attorney General determines poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the federal government, including insights regarding facilities, activities, or populations in those locations, to the detriment of national security, because of the nature of those locations or the personnel who work there. "Government-related data" also includes any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and intelligence community.

Prohibited, Restricted, and Exempt Transactions

Prohibited Transactions

As discussed in further detail below, the Final Rule prohibits certain transactions involving data brokerage and all covered data transactions involving bulk human 'omic data.

No U.S. person may, on or after April 8, 2025, knowingly[16] engage in a covered data transaction involving data brokerage with a country of concern or covered person, unless an exemption or license applies. Data brokerage is defined as the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person to any other person, where the recipient did not collect or process the data directly from the individuals linked or linkable[17] to the collected or processed data.

In addition, no U.S. person may, on or after April 8, 2025, knowingly engage in any covered data

definition of a "trade secret" (as defined in 18 U.S.C. § 1839(3)) or "proprietary information" (as defined in 50 U.S.C. § 1708(d)(7));
(2) Data that is, at the time of the transaction, 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, which means any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value, as set out under 50 U.S.C. § 1702(b)(1); and
(4) Information or informational materials (as further defined in the Final Rule) and ordinarily associated metadata or metadata reasonably necessary to enable the transmission or dissemination of such information or informational materials.

[15] Such thresholds include:

- Human 'omic data collected about or maintained on more than 1,000 U.S. persons, or, in the case of human genomic data, more than 100 U.S. persons;
- Biometric identifiers collected about or maintained on more than 1,000 U.S. persons;
- Precise geolocation data collected about or maintained on more than 1,000 U.S. devices;
- Personal health data collected about or maintained on more than 10,000 U.S. persons;
- Personal financial data collected about or maintained on more than 10,000 U.S. persons;
- Covered personal identifiers collected about or maintained on more than 100,000 U.S. persons; or
- Combined data, meaning any collection or set of data that contains more than one of the categories above, or that contains any listed identifier linked to the categories above, 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.

[16] "Knowingly" with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result.

[17] "Linked" means associated, and the term "linkable" means reasonably capable of being linked.

transaction that involves any access by a foreign person to government-related data or bulk U.S. sensitive personal data and that involves data brokerage with any foreign person that is not a covered person unless the U.S. person (1) contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement in accordance with the reporting requirements of the Final Rule.

Further, no U.S. person may, on or after April 8, 2025, knowingly engage in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human 'omic data (as defined above), or to "human biospecimens"[18] from which bulk human 'omic data could be derived.

Finally, no U.S. person, on or after April 8, 2025, may enter into a transaction for the purpose of evading, avoiding, causing a violation of, or attempting to violate the Final Rule, and no U.S. person may knowingly direct[19] a covered data transaction that would be prohibited if engaged in by a U.S. person.

Restricted Transactions

Restricted transactions are not prohibited, but U.S. persons engaging in such transactions must satisfy certain requirements.

Specifically, no U.S. person may, on or after April 8, 2025, knowingly engage in a covered data transaction involving a vendor agreement,[20] employment agreement,[21] or investment agreement[22] (*i.e.*, not a data-brokerage transaction) with a country of concern or covered person unless the U.S. person complies with certain security requirements.

The applicable security requirements[23] are divided into two broad categories: (i) organizational- and system-level requirements and (ii) data-level requirements. The organizational- and system-level requirements require certain organizational cybersecurity policies, access controls like multifactor authentication, and periodic data risk assessments. The data-level requirements include mitigation measures like data minimization, data masking, encryption, privacy-enhancing technologies, and access management to prevent unauthorized access to sensitive data by covered persons or countries of concern.

Exempt Transactions

Certain types of transactions are exempt under the Final Rule. An exempt transaction is a transaction that is otherwise a covered data transaction but that is

[18] Human biospecimens means a quantity of tissue, blood, urine, or other human-derived material, including such material classified under certain 10-digit Harmonized System-based Schedule B numbers.

[19] "Knowingly" with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result; and "directing" means having any authority (individually or as part of a group) to make decisions for or on behalf of an entity and exercising that authority.

[20] A vendor agreement is any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.

[21] An employment agreement is any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

[22] An investment agreement is an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (i) real estate located in the United States; or (ii) a U.S. legal entity.

[23] The security requirements are not explicitly set forth in the Final Rule. Instead, the Final Rule incorporates by reference a separate rulemaking from the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, available here.

permissible because it qualifies for one of the following exemptions.

— **Personal Communications**: transactions involving postal, telegraphic, telephonic, or other personal communication that do not involve the transfer of anything of value.

— **Information or Informational Materials**: transactions involving the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.[24]

— **Travel**: transactions that are ordinarily incident to travel to or from any country.

— **Official Business of the United States Government**: transactions that are for the conduct of the official business of the U.S. Government by its employees, grantees, or contractors; any authorized activity of any U.S. Government department or agency; or transactions conducted pursuant to a grant, contract, or other agreement entered into with the U.S. Government.

— **Financial Services**: transactions that are ordinarily incident to and part of the provision of financial services.[25]

[24] The term "information or informational materials" is limited to expressive material and includes publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. It does not include data that is technical, functional, or otherwise non-expressive. Additionally, the term does not include:

(1) Information or informational materials not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials;
(2) Items that were, as of April 30, 1994, or that thereafter become, controlled for export to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by 18 U.S.C. chapter 37.

[25] Financial services include the following:

- **Banking and Financial Services**: banking, capital-markets (including investment-management services as well as trading and underwriting of securities, commodities, and derivatives), or financial-insurance services;
- **National Bank Financial Activities**: a financial activity authorized for national banks by 12 U.S.C. § 24 and rules and regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;
- **Financial Activities under the Bank Holding Company Act**: 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;
- **Transfer of Financial Data in Commerce**: 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);
- **Payment and Funds Transfer Services**: 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
- **Investment Management Services**: 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 or futures commission merchants executing trades within an

— **Corporate Group Transactions**: transactions 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 ordinarily incident to and part of administrative or ancillary business operations.[26]

— **Authorized by or Necessary for Compliance with Law**: transactions required or authorized by certain federal law or international agreements, or necessary for compliance with certain federal law.

— **CFIUS Action**: transactions involving an investment agreement subject to a CFIUS action.[27]

— **Telecommunications Services**: transactions, other than those involving data brokerage (as defined above), that are ordinarily incident to and part of the provision of telecommunications services.[28]

— **Drugs, Biological Products, and Medical Devices**: transactions that involve "regulatory approval data,"[29] and are necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or a combination product, provided that the U.S. person complies with the recordkeeping and reporting requirements set forth in the Final Rule.

— **Clinical Investigations and Post-Marketing Surveillance Data**: transactions that are ordinarily incident to and part of clinical

investment portfolio based upon instructions from an investment advisor).

[26] Administrative or ancillary business operations include:

- (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.

[27] The term "CFIUS action" means any agreement or condition the Committee on Foreign Investment in the United States has entered into or imposed pursuant to 50 U.S.C. § 4565(l)(1), (3), or (5) to resolve a national security risk involving access by a country of concern or covered person to sensitive personal data that the Committee on Foreign Investment in the United States has explicitly designated, in the agreement or document containing the condition, as a CFIUS action, including:

(a) Suspension of a proposed or pending transaction, as authorized under 50 U.S.C. § 4565(l)(1);

(b) Entry into or imposition of any agreement or condition with any party to a covered transaction, as authorized under 50 U.S.C. § 4565(l)(3); and
(c) The establishment of interim protections for covered transactions withdrawn before CFIUS's review or investigation is completed, as authorized under 50 U.S.C. § 4565(l)(5).

[28] "Telecommunications service" means the provision of voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol, wireless, fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming.

[29] "Regulatory approval data" means sensitive personal data that is de-identified or pseudonymized consistent with the standards of 21 C.F.R. § 314.80 and that is required to be submitted to a regulatory entity, or is required by a regulatory entity to be submitted to a covered person, to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product, including in relation to post-marketing studies and post-marketing product surveillance activities, and supplemental product applications for additional uses, where the terms "drug," "biological product," "device," and "combination product" have the meanings given to them in 21 U.S.C. § 321(g)(1), 42 U.S.C. § 262(i)(1), 21 U.S.C. § 321(h)(1), and 21 C.F.R. § 3.2(e), respectively.

investigations[30] or post-marketing surveillance data.[31]

Licenses and Advisory Opinions

The Final Rule authorizes DOJ to issue general and specific licenses. A general license will authorize transactions that meet the criteria specified in the general license, while a specific license will only authorize a particular transaction. DOJ plans to respond to all requests for specific licenses within 45 days of receipt. U.S. persons who avail themselves of a general license may be required to file reports and statements in accordance with the instructions specified in such licenses. Failure to do so may nullify the relevant authorization.

Under the Final Rule, U.S. persons involved in transactions potentially regulated by the Final Rule also can request an advisory opinion from the Attorney General. Such requests must relate to actual transactions with identified parties and focus on prospective conduct. DOJ may request additional information and conduct an investigation before issuing an advisory opinion. DOJ aims to respond to advisory opinion requests within 30 days of receipt.

Due Diligence, Audit, Reporting, and Recordkeeping Requirements

By October 6, 2025, U.S. persons engaging in any restricted transactions must develop and implement a written data compliance program that includes, among other elements: (1) risk-based procedures to verify data flows, including the types and volumes of bulk U.S. sensitive personal data or government-related data, the identities and ownership of transaction parties, and the end-use and transfer method; and (2) procedures to verify vendor identities. Starting October 6, 2025, U.S. persons involved in restricted transactions also must conduct an annual audit to ensure compliance with security requirements and other requirements under the Final Rule. The audit must be performed by a qualified, independent auditor who is not a covered person or a country of concern. The auditor must submit a written report within 60 days of completing the audit to the U.S. person. This report should detail the nature of the U.S. person's restricted transactions, the audit's methodology, the effectiveness of the data compliance program, any security vulnerabilities, and recommendations for improvement.

U.S. persons involved in transactions subject to the Final Rule must keep and maintain comprehensive records of each such transaction for at least 10 years.

In addition, beginning October 6, 2025, U.S. persons that are 25% or more owned by a country of concern or covered person and that are engaged in restricted cloud-computing transactions must file an annual report. Reports are due by March 1 each year, covering covered data transactions as of December 31 of the previous year.[32]

[30] "Clinical investigations" means a clinical investigation regulated by the U.S. Food and Drug Administration ("FDA") under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act ("FD&C Act") or clinical investigations that support applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, or infant formula, where the terms "drug," "biological product," "device," "combination product," and "infant formula" have the meanings given to them in 21 U.S.C. § 321(g)(1), 42 U.S.C. § 262(i)(1), 21 U.S.C. § 321(h)(1), 21 C.F.R. § 3.2(e), and 21 U.S.C. § 321(z) respectively.

[31] "Post-marketing surveillance data" means the collection or processing of clinical care data indicating real-world performance or safety of products, or the collection or processing of post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by the FDA, provided the data is de-identified or pseudonymized consistent with the standards of 21 C.F.R. § 314.80.

[32] The report must include:

- The U.S. person's name, address, and contact information;
- A description of the transaction, including the date, types of government-related data or bulk U.S. sensitive personal data and the volumes of each, data transfer method, and details of participants and their locations;
- Copies of relevant documentation; and
- Any additional information required by DOJ.

Further, any U.S. person who, on or after October 6, 2025, receives and affirmatively rejects an offer for a prohibited transaction involving data brokerage must file a report, unless prohibited by law. Reports must be filed with DOJ within 14 days of rejecting a prohibited transaction.[33]

The Final Rule provides DOJ with authority to conduct investigations, hold hearings, and require document production through subpoenas.

Penalties and Enforcement

Pursuant to the International Emergency Economic Powers Act ("IEEPA"), any violation, attempt to violate, conspiracy to violate, or causing a violation of any license, order, regulation, or prohibition issued under the Final Rule can result in civil penalties of up to $368,136 or twice the transaction amount involved in the violation and criminal penalties for willful violations of fines up to $1,000,000 and/or imprisonment for up to 20 years for individuals.

…

CLEARY GOTTLIEB

[33] The report must include the following information:

- The name and address of the rejecting U.S. person and contact details for further information; and
- A description of the rejected transaction, including:
  - Date of rejection;
  - Types and volumes of government-related data or bulk U.S. sensitive personal data involved;
  - Method of data transfer;
  - Details of participants and their locations, including data recipients and any countries of concern;
  - Relevant documentation; and
  - Any additional information required by DOJ.