PROGRAM MATERIALS
Program #36161
May 26, 2026

The Bulk Sensitive Data Rule: The First Year

- Julia Jacobson, Esq. - Squire Patton Boggs (US)
- Scott Warren, Esq. - Squire Patton Boggs (Toyko)

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

SQUIRE PATTON BOGGS

The Bulk Sensitive Data Rule:
The First Year

May 26, 2026 12:00PM EST

Speakers

SQUIRE PATTON BOGGS

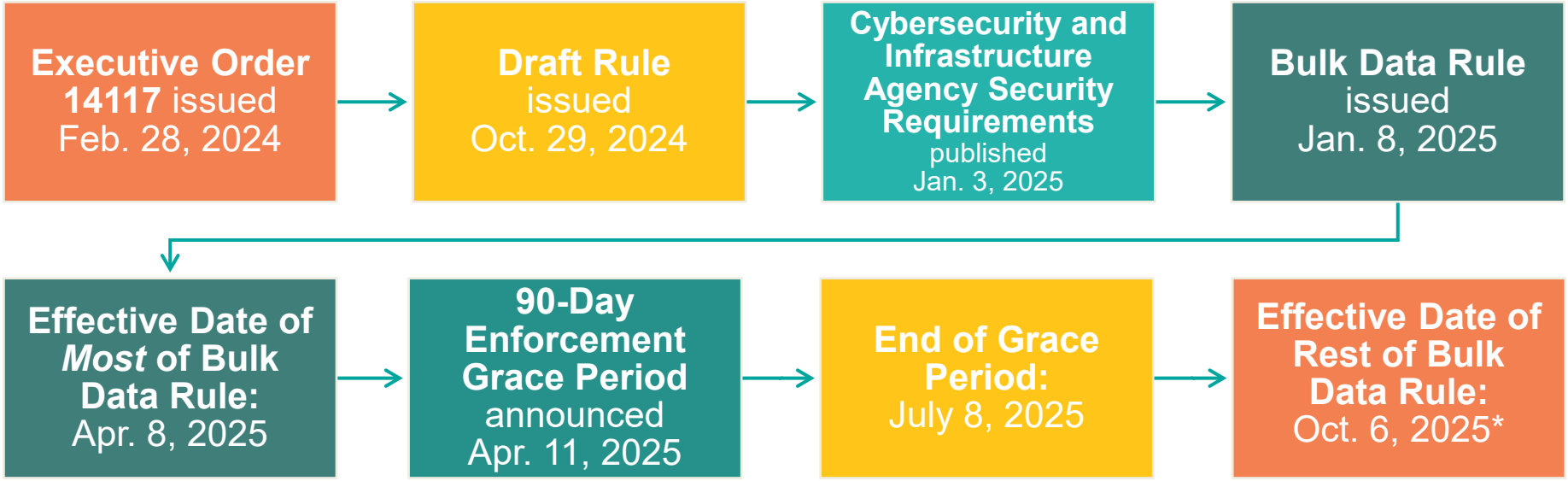
Julia Jacobson
Partner
Data Privacy, Cybersecurity & Digital Assets
(New York)
julia.jacobson@squirepb.com

Scott Warren
National Partner
Corporate
(Tokyo, Japan and Shanghai, China)
scott.warren@squirepb.com

SQUIRE PATTON BOGGS

The Bulk Data Rule Overview

Timeline



**Effective as of October 6, 2025: requirements for data compliance program; audits for restricted transactions; annual reports; and reports on rejected prohibited transactions.*

Executive Order 14117

SQUIRE PATTON BOGGS

"It is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an **unacceptable risk** to the **national security** of the United States."

"Unrestricted transfers of Americans' bulk sensitive personal data and United States Government-related data to such countries of concern may therefore enable them to **exploit such data for a variety of nefarious purposes**, including to engage in **malicious cyber-enabled activities**. Countries of concern can use their access to Americans' bulk sensitive personal data and United States Government-related data to **track and build profiles on United States individuals**, including Federal employees and contractors, for illicit purposes, including **blackmail and espionage**."

Industries particularly affected: financial services, health care, life sciences

“Bulk Data Rule”

SQUIRE PATTON BOGGS

Executive Order 14117: “The Attorney General, in consultation with the heads of relevant agencies, is authorized to take such actions, including the promulgation of **rules and regulations** … as may be necessary or appropriate to carry out the purposes of this order.”

October 29, 2024: the U.S. Department of Justice (***DOJ***) issued a *proposed* rule to implement Executive Order 14117.

January 8, 2025: the DOJ issued the *final* rule titled “Preventing Access to U.S. Sensitive Personal Data and Government Related Data by Countries or Concern or Covered Persons.” (***Bulk Data Rule***)

DOJ Guidance

SQUIRE PATTON BOGGS

On April 11, 2025, the DOJ issued **100 FAQs**, a "**Compliance Guide**" and an "**Implementation and Enforcement Policy through July 8, 2025**" (***DOJ Guidance***).[1]

- The stated purpose of the DOJ Guidance is to "assist individuals and entities in complying with legal requirements and to facilitate an understanding of the scope and purposes of the DSP."
  - In the DOJ Guidance, the Bulk Data Rule is called the "Data Security Program" or "DSP."
  - The National Security Division ("NSD") is the DOJ division that implements and enforces the Bulk Data Rule.
  - The DOJ implied that future guidance was forthcoming, e.g., "may separately issue DSP Enforcement Guidance to provide more information on violations of the DSP," but provided no indication about whether/when additional guidance will materialize.

On September 24, 2025, the DOJ added an FAQ (#106) regarding reporting a violation of the Bulk Data Rule (aka whistleblowing).

[1] See: https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive

Bulk Data Rule: Transaction Focus

SQUIRE PATTON BOGGS

The Bulk Data Rule is focused on *transactions*.

Each transaction requires analysis to determine whether it is a *covered data transaction*.

SQUIRE PATTON BOGGS

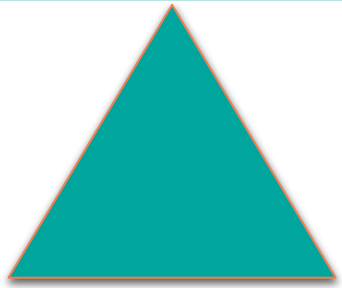
Covered Data Transactions

Covered Data Transaction

A ***covered data transaction*** means a transaction that involves access to “bulk U.S. sensitive personal data” or “government related data” by a “country of concern” or “covered person” and that involves “data brokerage; vendor agreement; employment agreement; or investment agreement.”

A covered data transaction is:

- a restricted transaction,
- a prohibited transaction, or
- an unauthorized restricted transaction



Analyzing Whether the Bulk Data Rule Applies

SQUIRE PATTON BOGGS

To start determining whether a data transaction is a covered data transaction, analyze these elements:

1. U.S. person knowingly engages in a data transaction involving
2. bulk U.S. sensitive personal data and/or government related data
3. that involves access
4. by a covered person or country of concern and
5. involves one of the four specified transaction types - a vendor agreement, employment agreement, investment agreement, or data brokerage

U.S. Person

SQUIRE PATTON BOGGS

Person:
individual or entity

foreign person:
any person that is not a U.S. person

U.S.person (§ 202.256)

- U.S. citizen, national, or lawful permanent resident
- U.S. refugee or asylee
- any entity organized *solely* under U.S. laws or any U.S. jurisdiction
- any person *in* the U.S.

U.S. Person: Examples

- A parent company is organized under the laws of a **country of concern** and has a subsidiary organized under **U.S. law**.
  - The subsidiary is a U.S. person regardless of the degree of ownership by the parent company; *the parent company is a foreign person*.

- A parent company is organized under **U.S. law** and has a subsidiary organized under the law of a **country of concern**.
  - The subsidiary is a foreign person regardless of the degree of ownership by the parent company; *the parent company is a U.S. person.*

“Knowingly”

SQUIRE PATTON BOGGS

A U.S. person who or that *knowingly* engages in or directs a covered data transaction.

- ***knowingly*** (§ 202.230) means a person “has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result”
  - ‘engages’ and ‘directs’ are not defined terms
- The DOJ will “consider relevant facts and circumstances, including the sophistication of the individual or entity, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction appeared to be aware”

Country of Concern

SQUIRE PATTON BOGGS

"**country of concern**" (***CoC***)(§ 202.209) means:

- China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela

Plus, the DOJ has the authority to identify any other foreign government that it determines has engaged in a long-term pattern or serious instances of conduct significantly adverse to U.S. national security and poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of U.S. national security.

Covered Person

SQUIRE PATTON BOGGS

"**covered person**" (***CP***) (§ 202.211(1)-(4)) means:

1. foreign entity ≥ 50% *owned** by a CoC
2. foreign entity *organized* under a CoC's laws
3. foreign entity with a *principal place of business* in a CoC
4. foreign entity ≥ 50% *owned** by *another CP*
5. foreign *employee/contractor* of CoC or CP (entity)
6. foreign individual who *resides primarily* in a CoC

**owned = directly or indirectly, individually or in aggregate*

Examples: Covered Person

SQUIRE PATTON BOGGS

- A Chinese citizen located in the U.S. is a U.S. person, not a CP (unless he/she is individually designated), and is subject to the same prohibitions and restrictions as other U.S. persons with respect to engaging in covered data transactions with a CoC or CP.

- A citizen of a CoC who is primarily a resident of a third country (i.e., not a CoC) is not a CP unless he/she is individually designated or is an employee or contractor of a CoC government or a CP entity.

- A foreign person is located abroad and is employed by a company headquartered in a CoC. Because the company is a CP and the employee is located outside the U.S., the employee is a CP.

Covered Person

SQUIRE PATTON BOGGS

"The term *covered person* means:
[…] any person anywhere as determined by the DOJ:
(i) *To be, to have been, or to be likely to become owned or controlled* by or subject to the jurisdiction or direction of a country of concern or covered person; (ii) To act, to have acted or purported to act, or to be likely to *act for or on behalf of a country of concern or covered person*; or (iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation …" (§ 202.211(5))

Covered Person

SQUIRE PATTON BOGGS

§ 202.211(5)

Per commentary: “a controlling interest may present risks of access, which is why control is one of the criteria for the Department to designate an entity as a covered person under § 202.211(a)(5) […] U.S. persons should exercise caution when considering engaging in covered data transactions with an entity that is not a covered person but in which one or more covered persons have significant ownership that is less than 50 percent, or which one or more covered persons may control by means other than a majority ownership interest.”

The DOJ will add any designated CP to its Covered Persons List (accessible through the NSD’s website). Designated CPs remain CPs even when located in the United States.

Access

SQUIRE PATTON BOGGS

"**access**" (§ 202.201) 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 [which is] determined ***without regard for the application or effect of any security requirements***

The Data

SQUIRE PATTON BOGGS

sensitive personal data (***SPD***) (§ 202.249) means "covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof"

bulk U.S. sensitive personal data (***U.S. SPD***) (§ 202.206) means "a collection or set of sensitive personal data relating to U.S. persons, in any format, *regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted*," if the data meets or exceeds the bulk thresholds

- *Consent is not a factor*

SPD Categories

SQUIRE PATTON BOGGS

Sensitive Personal Data Categories	Definition
(a) Human ’omic data	human genomic data, human epigenomic data, human proteomic data, human transcriptomic data
(b) Biometric identifiers	measurable physical characteristics or behaviors used to recognize or verify the identity of an individual
(c) Precise geolocation data	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
(d) Personal health data	health information that indicates, reveals, or describes the past, present, or future physical or mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to the individual

SPD Categories

Sensitive Personal Data Categories	Definition
(e) Personal financial data	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 consumer report
(f) Covered personal identifiers (§ 202.212)	any ***listed identifier*** *[discussed below]* in combination with (i) any other listed identifier; or (ii) other data disclosed by a transacting party pursuant to the transaction if the listed identifier *is linked or linkable to other listed identifiers or to other sensitive personal data* [*see next slide*]
(g) Combined data	data set that contains more than one SPD category or that contains any listed identifier linked to SPD category that in the aggregate meets the lowest bulk threshold [*Element 5 below*]

Not SPD

SQUIRE PATTON BOGGS

- Data that does not relate to an individual
  - e.g., trade secrets
- Data lawfully available to the public from publicly available federal/state/local government records
  - e.g., court records
- Data lawfully available to the public in widely distributed media
  - e.g., databases freely available to the scientific community
- Personal Communications
- “Information or informational materials” that are “expressive” and associated metadata – n.b., not as broad as it seems
  - e.g., online posting/publication of health-related research data by individual researchers

Listed Identifier

listed identifier (§ 202.234) means any piece of data in any of the following data fields:

a) Full or truncated government identification or account number (such as a Social Security number, driver's license or State identification number, passport number, or Alien Registration Number);
b) Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company;
c) Device-based or hardware-based identifier (such as International Mobile Equipment Identity (“IMEI”), Media Access Control (“MAC”) address, or Subscriber Identity Module (“SIM”) card number);
d) Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);
e) Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (“MAID”));
f) Account-authentication data (such as account username, account password, or an answer to security questions);
g) Network-based identifier (such as Internet Protocol (“IP”) address or cookie data); or
h) Call-detail data (such as Customer Proprietary Network Information (“CPNI”)).

Not Covered Personal Identifiers

SQUIRE PATTON BOGGS

- 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

- 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

“Bulk”

SQUIRE PATTON BOGGS

bulk (§ 202.205) means any amount of sensitive personal data that meets or exceeds the 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

Sensitive Personal Data Category	Bulk Threshold for any covered data transaction initiated, pending or completed on or after April 8, 2025
Human ’omic data	1,000 U.S. persons or 100 U.S. persons for genomic data
Biometric identifiers	1,000 U.S. persons
Precise geolocation data	1,000 U.S. devices
Personal health data	10,000 U.S. persons
Personal financial data	10,000 U.S. persons
Covered personal identifiers	100,000 U.S. persons
Combined data	Lowest applicable threshold of U.S. persons or U.S. devices for any SPD category

Government Related Data

government related data (§ 202.222) means (i) precise geolocation data, regardless of volume, for any location within any area on the Government-Related Location Data List* or (ii) any sensitive personal data, regardless of volume, that a transacting party *markets* as linked or linkable to current or recent former employees, contractors, or senior officials of the U.S. government

*Government-Related Location Data List means the list of latitude/longitude coordinates of geofenced areas which include the worksite or duty station of Federal Government employees or contractors who occupy a national security position, military installations (commonly known Department of Defense sites), or homeport facilities for any ship, ranges, and training areas in the United States and its territories, as supplemented from time to time

Four Transaction Types

SQUIRE PATTON BOGGS

1. **data brokerage** means sale, licensing, or similar commercial transaction involving covered data and a CoC or CP (*but excluding 2. – 4. below)* and that involves the transfer of data from any person (the initiator) to any other person (the recipient) if the *recipient* did not collect or process the data directly from the individuals linked or linkable to the collected or processed data
2. **vendor agreement** means an agreement/arrangement in which a person provides goods or services to another person for payment or other consideration (excluding an employment agreement)
3. **employment agreement** means an agreement in which an individual performs work for another person in exchange for payment or other consideration (n.b., not an independent contractor arrangement)
4. **investment agreement** means an agreement in which any *person* in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to U.S. real estate or a U.S. legal entity (excluding “certain passive investments”)

SQUIRE PATTON BOGGS

Prohibited Transaction and Restricted Transaction

Covered Data Transactions are either Prohibited or Restricted

SQUIRE PATTON BOGGS

Prohibited Transaction

Five (5) categories of **prohibited** transactions

- data transaction is not prohibited if exempt or licensed.

Restricted Transaction

A data transaction that involves a:

- vendor agreement
- employment agreement
- investment agreement

… but only if compliance and security requirements are met.

Prohibited Transactions: 5 Categories

prohibited transaction (§ 202.243) means a "data transaction that is subject to one or more of the prohibitions described in subpart C of this part."

Subpart C's 5 Categories (§§ 202.301 – 202.305)

1. U.S. persons knowingly engaging in a covered data transaction involving **data brokerage** with a CoC or CP (§ 202.301)
2. U.S. persons knowingly engaging in a covered data transaction involving **data brokerage** with a foreign person **(that is not a CP)** *unless* the U.S. person (1) contractually requires that the foreign person refrain from onward sale with a CoC or CP; and (2) reports any known or suspected violations of the contractual requirement (§ 202.302)

Prohibited Transactions: 5 Categories, *continued*

SQUIRE PATTON BOGGS

3. U.S. persons knowingly engaging in a covered data transaction with a CoC or CP that involves access by that CoC or CP to **bulk human 'omic data** or to human biospecimens from which bulk human 'omic data could be derived (§ 202.303)
4. Transaction with the **purpose of evading or avoiding**, that **causes a violation** of, or attempts to violate any of the prohibitions set forth in the Bulk Data Rule or any **conspiracy** formed to violate the prohibitions in the Bulk Data Rule (§ 202.304)
5. U.S. person **knowingly directing** any covered data transaction that would be a prohibited transaction or unauthorized restricted transaction if engaged in by a U.S. person (§ 202.305)

Examples: Prohibited Transactions

SQUIRE PATTON BOGGS

- A U.S. company owns or operates a mobile app or website for U.S. users. That mobile app or website contains one or more tracking pixels or software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. The tracking pixels or software development kits transfer or otherwise provide access to government-related data or bulk U.S. sensitive personal data to a CoC or CP-owned social media app for targeted advertising. The U.S. company engages in prohibited data brokerage that would be a prohibited transaction.

- A U.S. company that conducts consumer human genomic testing collects and maintains bulk human genomic data from U.S. consumers. The U.S. company has global IT operations, including employing a team of individuals who are citizens of and primarily resident in a CoC to provide back-end services. The agreements related to employing these individuals are employment agreements. Employment as part of the global IT operations team includes access to the U.S. company's systems containing the bulk human genomic data. These employment agreements would be prohibited transactions (because they involve access to bulk human genomic data).

Examples: Restricted Transactions

SQUIRE PATTON BOGGS

✓ A U.S. company engages in an employment agreement with a CP to provide information technology support. As part of their employment, the CP has access to personal financial data. The U.S. company implements and complies with the security requirements. The employment agreement is authorized as a restricted transaction because the company has complied with the security requirements.

X A U.S. company engages in a vendor agreement with a CP to store bulk personal health data. Instead of implementing the security requirements in the Bulk Data Rule, the U.S. company implements different controls that it believes mitigate the CP's access to the bulk personal health data. Because the U.S. person has not complied with the security requirements, the vendor agreement is not authorized and is a prohibited transaction.

Exempt Transaction Categories

SQUIRE PATTON BOGGS

"**exempt transaction**" means a data transaction that is subject to one or more exemptions (§202.501 – §202.511 – 11 categories). All requirements of the specific exemption applied to the transaction must be met to qualify.

- Personal communications: exempt if involve postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value
- Telecommunications services: other than data brokerage, exempt if *ordinarily incident* to/part of provision of telecommunications services
- Information or informational materials: exempt if involve the importation/exportation from/to any country, whether commercial or otherwise, regardless of how transmitted
- Travel: exempt if *ordinarily incident* to travel to/from any country
- Financial services: exempt if *ordinarily incident* to and part of the provision of financial services

Exempt Transaction Categories, *continued*

SQUIRE PATTON BOGGS

- Corporate group transaction: exempt if transaction between a U.S. person and its foreign subsidiary or affiliate is **ordinarily incident** to and part of administrative or ancillary business operations
- Transactions required/authorized or necessary for compliance with Federal law
- Official U.S. Government Business: exemption includes transactions conducted pursuant to a U.S. Government grant, contract, or other agreement
- Investment agreements subject to a CFIUS action
- Drug, Biological Product, and Medical Device authorizations
- Other Clinical Investigations and Post-Marketing Surveillance Data: subject to "ordinarily incident" requirements

Exempt Transaction Category: Corporate Group Transaction

SQUIRE PATTON BOGGS

Ordinarily incident to and part of administrative or ancillary business operations includes:

i. Human resources
ii. Payroll, expense monitoring/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
x. Employees' internal and external communications

Licensed Transactions

SQUIRE PATTON BOGGS

general license (§ 202.231(a)) means a written license authorizing a class of transactions and *not limited to a particular person* – published in the Federal Register but "issued only in rare circumstances as the [DOJ] deems appropriate"

specific license (§ 202.231(b)) means a written license issued authorizing a particular transaction or transactions *in response to a written license application* - authorizes one or more transactions that would otherwise be prohibited but only for the parties that applied

- DOJ will "endeavor" to issue licensing decisions within 45 days after all information necessary to make a licensing decision is received from the parties.

A license will not apply to a prior transaction unless license specifically provides.

All requirements of the license must be met to be a licensed transaction, not a CDT.

Restricted Transactions: Security Requirements

SQUIRE PATTON BOGGS

Cybersecurity and Infrastructure Agency (CISA) Security Requirements published on January 3, 2025

1. Organizational and System Level Requirements
   - Ensure basic organizational cybersecurity policies, practices, and requirements
   - Implement logical and physical access controls to prevent CPs or CoCs from gaining access to covered data
   - Conduct an internal data risk assessment that evaluates whether and how the overall approach selected and implemented sufficiently prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by CPs and/or CoCs

2. Data-Level Requirements
   - Apply data minimization and data masking strategies
   - Apply encryption techniques
   - Apply privacy enhancing technologies
   - Configure identity and access management to deny authorized access to covered data by CPs and CoCs within all covered systems

Restricted Transactions: Data Compliance Program Requirements

SQUIRE PATTON BOGGS

- Risk-Based Procedures – establish and implement risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner, the following:
  - the types and volumes of bulk U.S. sensitive personal data or government-related data involved in any restricted transactions
  - the identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals
  - the end-use of the data and the method of data transfer
- Vendor Management and Validation – for restricted transactions that involve vendor agreements, the Data Compliance Program must include risk-based procedures for verifying the identity of vendors; specifically, U.S. persons should screen vendors to verify whether current or prospective vendors are CPs
- Written Data Compliance Program Policy – a written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance

Restricted Transactions: Data Compliance Program Requirements, *continued*

SQUIRE PATTON BOGGS

- Written Security Requirements Policy – a written policy that describes the implementation of the security requirements and is annually certified by an officer, executive, or other employee responsible for compliance
- Audit Requirements
  - U.S. person must undertake an *independent* audit of compliance with Security Requirements, Data Compliance Program, and Records
  - One audit for each *calendar* year in which the U.S. person engages in any restricted transaction that covers the *12 months* preceding the restricted transaction
  - Independent auditor must submit report to U.S. person's senior officer within 60 days after completion; U.S. person must retain for 10 years
- Recommendation in DOJ Guidance: Training Personnel – "consider providing periodic (ideally, at least annual) training on the Data Compliance Program and the Security Requirements to all relevant employees and personnel"

“Know Your Data”

SQUIRE PATTON BOGGS

- KYD requirements (FAQ 79):
  - “specifically require that U.S. persons engaging in restricted transactions develop and implement data compliance programs with risk-based procedures for verifying data transactions, including the types and volumes of data involved in the transactions, the identity of the transaction parties, and the end-use of the data.”
  - generally, as part of a risk-based compliance program, “DOJ expects “U.S. individuals and entities to take reasonable steps to know their data when they are dealing in government-related data and bulk U.S. sensitive personal data. Companies choosing to engage in these categories of data transactions can and should have awareness of the volume and types of data they possess and in which they are transacting.”

Recordkeeping and Reporting Requirements

SQUIRE PATTON BOGGS

Recordkeeping – *a U.S. person* engaging in any data transaction "must keep a full and accurate record of each such transaction that is available for examination for at least 10 years after the date of the transaction" (§ 202.1101(a))

Reporting – *every person* engaged in *any* act or transaction or covered data transaction subject to the Bulk Data Rule is required to "furnish under oath, in the form of reports or otherwise, from time to time and at any time as may be required" by the DOJ, information relative to the act, transaction, or covered data transaction, regardless of whether "effected pursuant to a license or otherwise "(§ 202.1102)

Restricted Transaction: Recordkeeping and Reporting Requirements

SQUIRE PATTON BOGGS

Annual Certification (§ 202.1101(b)) - an officer, executive, or other employee responsible for compliance must sign an annual certification of:

- Data Compliance Program implementation and due diligence efforts
- implementation of CISA requirements
- the completeness and accuracy of recordkeeping documenting due diligence, as supported by an audit

Annual Report (§ 202.1103) - any U.S. person that, on or after October 6, 2025, is engaged in a restricted transaction involving *cloud-computing services*, and that has 25% or more of the U.S. person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a CoC or CP, must file an annual report

Restricted Transaction: Recordkeeping Exclusions

SQUIRE PATTON BOGGS

The recordkeeping requirements do not apply to a covered data transaction subject to one of the following exemptions:

- corporate group transactions
- transactions required or authorized by Federal law or international agreements, or necessary to comply with Federal law
- investment agreements subject to a CFIUS action
- telecommunications services

Reports on Rejected Prohibited Transactions

SQUIRE PATTON BOGGS

- A report must be filed, except as otherwise prohibited by Federal law, by any U.S. person that, on or after October 6, 2025, has received and affirmatively rejected (including automatically rejected using software, technology, or automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage.
  - The report must be filed within 14 days after a suspected violation or after becoming aware of an actual violation.

SQUIRE PATTON BOGGS

Consequences of Non-Compliance

Consequences of Non-Compliance

SQUIRE PATTON BOGGS

- Civil penalties of up to the greater of $368,136 or twice the value of each violative transaction.
- Willful violations are punishable by imprisonment of up to 20 years and a $1,000,000 fine.
  - criminal penalties apply if any person “knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry” (§ 28 CFR 202.1301(a)(3))
- Individuals (U.S. and outside U.S.) reporting violations may be eligible for financial incentives if reported through FinCEN’s whistleblower program.

Whistleblower Rewards

SQUIRE PATTON BOGGS

- FinCEN Whistleblower Program
- A reporting individual ("whistleblower") is eligible for a FinCEN whistleblower reward if the individual provides "original information" about violations of IEEPA that lead to a successful enforcement action that results in monetary sanctions of more than $1 million.
  - The term "original information" means that the information is derived from the whistleblower's independent knowledge and is not known from another source. 31 U.S.C. § 5323(a)(3).
  - The term "monetary sanctions" means "any monies, including penalties, disgorgement, and interest, ordered to be paid; and (B) does not include (i) forfeiture; (ii) restitution; or (iii) any victim compensation payment." 31 U.S. Code § 5323(a)(2).

Whistleblower Rewards

SQUIRE PATTON BOGGS

Another option for violations by a public company

- The Securities and Exchange Commission (***SEC***) also has a whistleblower rewards program that covers an individual (or group of individuals) who is a contractor or subcontractor of a public company and who reports "original information" that relates to a possible violation of the federal securities laws (including any SEC rule or regulation) that has occurred, is ongoing, or is about to occur. 17 C.F.R. § 240.21F–2(a)(2).
- The SEC must reward the whistleblower when the whistleblower's original information leads to a successful enforcement in which the SEC obtains monetary sanctions of more than $1 million. The term "monetary sanctions" means an SEC order to pay money designated as penalties, disgorgement, or interest or as relief for the violations, such as restitution in a criminal proceeding or monies returned to harmed investors. 17 CFR § 240.21F-5(c).

SQUIRE PATTON BOGGS

Vendors and Covered Data Transactions

Assessing Vendors

SQUIRE PATTON BOGGS

The DOJ expects that a U.S. person will conduct "reasonable" and "affirmative" due diligence to "know your data" (*KYD*). (FAQ 79)

Per DOJ's April 11, 2025 Compliance Guide, KYD includes knowing:

- the kinds and volumes of data that the U.S. person (entity/company) collected about or maintained on U.S. persons or U.S. devices
- how U.S. person (entity/company) uses the data
- whether the U.S. person (entity/company) engages in covered data transactions
- identity of the transaction parties
- how the U.S. person (entity/company) markets data

Know Your Data - Vendors

SQUIRE PATTON BOGGS

To KYD, the U.S. person (entity/company) needs to (at least):

- ❑ Determine what vendors have access to its U.S. SPD or GRD
- ❑ Verify the identity of each vendor, including screening the vendor against the Covered Persons List (once published) (FAQ 91)
- ❑ Determine whether a vendor is based in, has offices in, or operates in a CoC or has other indicia of covered person status
- ❑ Determine whether a vendor is a foreign person
- ❑ Determine whether a data transaction with a foreign person involves data brokerage

But …

Know Your Data - Vendors

SQUIRE PATTON BOGGS

"Second-level" Diligence Is Not Required

"U.S. persons engaging in vendor agreements … with foreign persons are generally not expected to conduct due diligence on the employment practices of those foreign persons to determine whether their employees qualify as covered persons. Generally, a U.S. person has not knowingly directed a restricted transaction where that U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person and that foreign person, in turn, employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. It may, however, constitute a DSP violation for that U.S. person to knowingly direct that foreign person company to enter an employment agreement with that covered person to indirectly accomplish what would otherwise be a prohibited or restricted transaction if engaged in directly by the U.S. person…" (Compliance Guide, Section IV)

Vendor Contracts

SQUIRE PATTON BOGGS

The Bulk Data Rule and the guidance do not provide general vendor contractual requirements, like other privacy/security laws (*but see slide 53 for data brokerage*)

Possible contractual terms to avoid the Bulk Data Rule

Vendor warrants that:

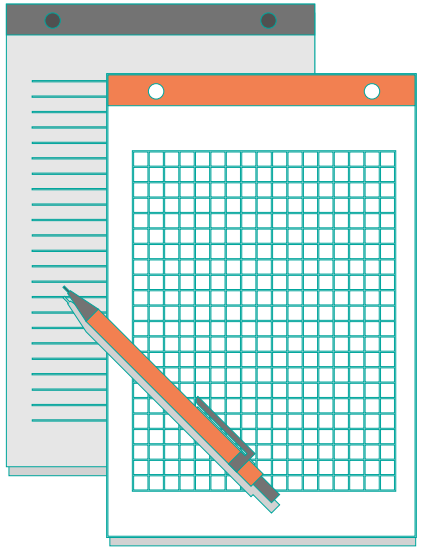
- it and its personnel are not CPs and will notify customer if that changes
- it will not permit a covered person or "foreign person" to access in any manner any of the U.S. person customer's data (even if the data is anonymized, pseudonymized, de-identified, or encrypted) without express prior written consent
- it will not engage in any activity that causes or is reasonably likely to cause any of the requirements of the Bulk Data Rule to apply to the customer

Vendor Contracts

SQUIRE PATTON BOGGS

Possible contractual terms for a Restricted Transaction:

- vendor warrants compliance with CISA's security requirements
- vendor will not allow a CP or CoC to directly or indirectly access customer's data
- vendor will participate in an audit by customer's independent auditor if needed for customer's audit required by § 202.1002
- vendor will, upon request, provide customer with information to demonstrate compliance with the Bulk Data Rule



Vendor Contracts – Data Brokerage with Foreign Persons

SQUIRE PATTON BOGGS

For data brokerage with a foreign person, the U.S. person must take certain steps to address the risk of an onward transfer of U.S. SPD and GRD by the foreign person to a CoC or CP, including:

1. contractual terms in which the foreign person agrees not to resell or give access to a CoC or CP to the U.S. SPD and GRD – sample language provided in Compliance Guide Section III.B.1 but not mandatory
2. disclosing known or suspected violations of the contractual terms

(§ 202.302(a), FAQ 62)

Distinguishing Protecting Americans' Data from Foreign Adversaries Act

SQUIRE PATTON BOGGS

Protecting Americans' Data from Foreign Adversaries Act (PADFAA) prohibits:

a "data broker to sell" or "otherwise make available personally identifiable sensitive data of a United States individual" to any foreign adversary country or any entity that is controlled by a foreign adversary.

- The key difference is the consent-based exception.
- Enforced by the FTC

SQUIRE PATTON BOGGS

Bulk Data Rule: What's Happening Now

The Bulk Data Rule in Lawsuits

SQUIRE PATTON BOGGS

On September 2, 2025, two class action lawsuits were filed in federal district court that alleged adtech providers (Xandr, Inc. and Index Exchange, Inc.) violated the Electronic Communications Privacy Act (***ECPA***) because they breached the Bulk Data Rule by sharing data with a "covered person."

The definition of data brokerage "covers both first-party data brokerage (by the person that directly collected the U.S. person's data) and third-party data brokerage (by a person that did not directly collect the U.S. person's data, such as a subsequent reseller)." (Bulk Data Rule FAQ 18)

The broad definition means that whether a company considers itself a data broker or not, the Bulk Data Rule may apply.

The Bulk Data Rule in Lawsuits

SQUIRE PATTON BOGGS

- Other class action complaints:
  - *Christy V. Lenovo Inc*. – filed February 5, 2026
  - *Malko v. GNC Holdings, LLC* – filed February 20, 2026
  - *Hsu v. Fantasia Trading LLC (Anker)* – filed March 4, 2026
  - Three class action complaints filed against Google - February 19, 2026

- On February 19, 2026, three class action complaints were filed against Google
- The complaints alleged that Google combined users' IP addresses and other network-level signals with cookie data and persistent advertising identifiers, and transferred such data to third parties, such as Pangle, MediaGo, and Temu.

The Bulk Data Rule in Lawsuits

SQUIRE PATTON BOGGS

- All eight cases focus on:
  1. The transfer of cookie and other marketing data
     - Types of data transferred include: IP addresses, advertising IDs, cookie data, full URLs, page titles, content of the page, device IDs, and user behavioral signals
  2. Lack of user consent
     - Not providing (i) clear and conspicuous notice and (ii) a reasonable means to detect, prevent, or opt-out of collection and sharing
- These lawsuits allege that the interception and use of private communications through tracking technologies is a “criminal and tortious act”
- Violations of the ECPA provide a private right of action of $10,000 per violation if done for the purpose of committing “criminal or tortious acts”

SQUIRE PATTON BOGGS

Uplifting Compliance Policies and Procedures

Compliance Requirements – Restricted Transactions

SQUIRE PATTON BOGGS

- Security Requirements – CISA
- Data Compliance Program
- Recordkeeping
- Reporting
- Annual Compliance Certification by Senior Management and Compliance Personnel
- Annual Report for U.S. Persons engaged in certain restricted transactions involving cloud-computing services

Assessing Current Compliance

SQUIRE PATTON BOGGS

- Know the data categories the business collects and/or maintains about U.S. Persons and the volume of each category.
- Determine whether any of the data categories that the business collects or maintains are in-scope for the Bulk Data Rule, i.e., U.S. SPD or government-related data + meet the bulk threshold.
  - **Reminder**: Even anonymized, pseudonymized, de-identified, or encrypted data is in scope of the Bulk Data Rule.
- Determine how the business uses the in-scope data:
  - Does the business engage in one or more covered data transactions with CPs or CoCs?
  - Are the transactions prohibited or restricted?
  - Review vendor agreements and employment contracts.

Assessing Current Compliance

- Assess existing compliance programs:
  - For restricted transactions – gap-assess existing practices against Data Compliance Program and Security Requirements.
  - Incorporate a Data Compliance Program and the CISA Requirements into the business's broader data privacy program.
- Assess recordkeeping and procedures to meet reporting and audit requirements in Bulk Data Rule for restricted and prohibited transactions.
- Assess vendor screening procedures.

SQUIRE PATTON BOGGS

Wrap-Up

Wrapping Up

SQUIRE PATTON BOGGS

- Assess the application of the Bulk Data Transfer Rule on data and data transactions
- Determine the steps necessary to comply with the Bulk Data Transfer Rule and document compliance efforts
- Prepare to respond to:
  - inquiries from customers, vendors, and US regulators about cross-border data flows and data storage/localization
  - class action lawsuits

Questions?

JULIA JACOBSON
julia.jacobson@squirepb.com

SCOTT WARREN
scott.warren@squirepb.com

SPB Data Privacy Resources

SQUIRE PATTON BOGGS

Powered by SPB

Empower your data strategy with Squire Patton Boggs' comprehensive suite of privacy and cybersecurity tools — designed to help you navigate complex regulations and safeguard digital assets with confidence.

Privacy World Blog

Stay ahead of global data privacy trends with Privacy World Blog— your trusted source for expert analysis, legal updates, and practical guidance in an ever-evolving digital landscape.

Law & Policy Hub

Explore the future of law and technology at the Squire Patton Boggs AI Hub — your gateway to expert insights, legal innovation, and strategic guidance on artificial intelligence.

SQUIRE PATTON BOGGS

Appendix

Links to Source Materials

SQUIRE PATTON BOGGS

- Executive Order (EO) 14117 (Feb. 2024): https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related
- U.S. Department of Justice (*DOJ*) *proposed* rule to implement EO 14117: https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data
- DOJ Bulk Data Rule "Preventing Access to U.S. Sensitive Personal Data and Government Related Data by Countries or Concern or Covered Persons.": https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern
- DOJ's Press Release "Justice Department Implements Critical National Security Program To Protect Americans' Sensitive Data From Foreign Adversaries" - https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive
  - DOJ Data Security Program Compliance Guide (April 2025): https://www.justice.gov/opa/media/1396356/dl
  - DOJ Data Security Program – FAQs: https://www.justice.gov/opa/media/1396351/dl
  - DOJ Implementation and Enforcement Policy for First 90 Days: https://www.justice.gov/opa/media/1396346/dl?inline
- Security Requirements For Restricted Transactions E.O. 14117 Implementation: https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf

State Consumer Privacy Laws – Know Your Data

SQUIRE PATTON BOGGS

The Minnesota Consumer Data Privacy Act and the California Consumer Privacy Act (*CCPA*) Regulations specifically require documentation of data inventories. Other state consumer privacy laws have recordkeeping requirements.

- The Minnesota Consumer Data Privacy Act requires a controller to:
  - document data inventories (§ 325M.16(2)(c))
  - document and maintain a description of the policies and procedures specific to compliance with the Minnesota Consumer Data Privacy Act
    - includes reasonable administrative, technical, and physical data security practices

State Consumer Privacy Laws – Know Your Data

SQUIRE PATTON BOGGS

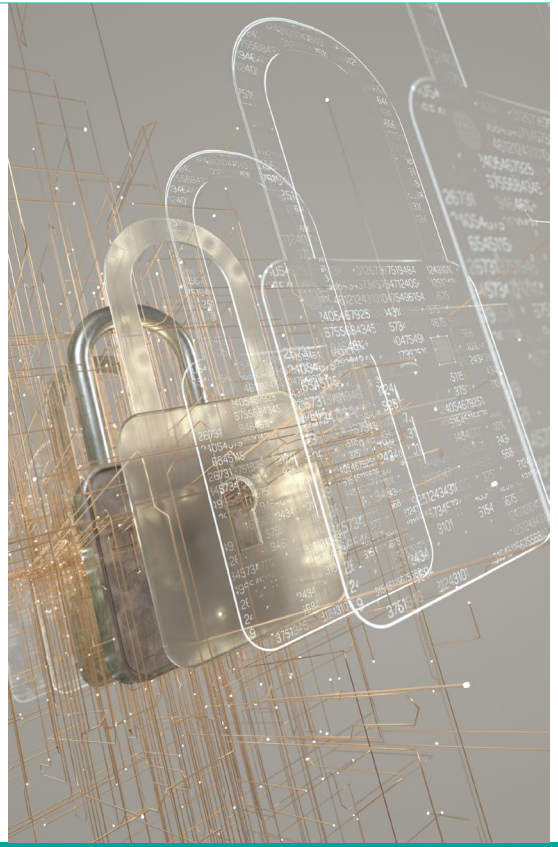
Knowing your data enables compliance with consumer privacy rights under the 20 state consumer privacy laws.

- Right to Access/Know: All require a controller to provide information about third-party recipients of personal data. Five (5) require a controller to provide a list of either specific third parties or categories of third parties that received personal data.
- Right to Correct: personal data: (i) that the consumer *provided to* the controller; (ii) *about* the consumer; or (iii) *provided by or obtained about* the consumer.
- Right to Delete: personal data: (i) *provided by or obtained about* the consumer; (ii) *concerning* the consumer; (iii) *about* the consumer; (iv) *collected from* the consumer; or (v) *provided to* the controller.
- Right to Data Portability: requires a controller to provide, in a usable format, copies of personal data: (i) *provided by* the consumer; (ii) *provided by or obtained about* the consumer; (iii) the consumer *previously provided;* or (iv) *processed* or *held* by the controller.
- Right to Opt-in/Opt-out: Of the processing of personal data for purposes of targeted advertising, sale, and profiling. Seven offer consumers the right to opt-out of profiling *in furtherance of solely automated decisions.*

CCPA Cybersecurity Audit Regulations

When a business's processing of consumer personal information "presents significant risk to consumers' security," the business must assess "the business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures)." (CCPA Regs § 7123(b))

- **Cybersecurity program** means "the policies, procedures, and practices that protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information." (CCPA Regs § 7001(k))



CCPA Cybersecurity Audit Regulations

SQUIRE PATTON BOGGS

As part of the audit, a business must assess its management of personal information, including:

- Personal information inventories (e.g., maps and flows identifying where personal information is stored, and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information); and
- Hardware and software inventories, and the use of allowlisting (i.e., discrete lists of authorized hardware and software to control what is permitted to connect to and execute on the business's information system)." (CCPA Regs § 7123(c)(4))

Massachusetts Data Security Law & Regulations

SQUIRE PATTON BOGGS

Massachusetts Data Security Law (Mass. Gen. Law Ch. 93H) is implemented by the "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth." (201 Mass. Code Regs. 17.00)

- Enacted in 2007, but still among the most prescriptive general state data security laws
- Requirements are qualified by whether they are "**technically feasible**," which means reasonable means through technology to accomplish the required result
- The Massachusetts data security regulations have **ten general minimum requirements** for a written information security program (**WISP**) and **eight computer security** minimum requirements

Tennessee Information Protection Act

SQUIRE PATTON BOGGS

The Tennessee Information Protection Act:

- requires that a controller "establish, implement, and maintain reasonable administrative, technical, and physical data security practices. . . to protect the confidentiality, integrity, and accessibility of personal information." (§ 47-18-3204(a)(3))
- provides a limited affirmative defense for violations if the controller's privacy program:
  - "reasonably conforms" to the National Institute of Standards and Technology Privacy Framework (***NIST***) or comparable privacy framework; and
  - is updated to "reasonably conform" with a subsequent revision to the NIST or comparable privacy framework within two (2) years of the publication date stated in the most recent revision. (§ 47-18-3213)