wiley

ALERT

FTC Sends Warning Letters to Data Brokers on PADFA Compliance

February 10, 2026

The Federal Trade Commission (FTC) announced it sent warning letters to 13 data brokers on February 9, 2026, cautioning them of requirements under the Protecting Americans' Data from Foreign Adversaries Act (PADFA) and urging a comprehensive review of their data practices. At a high level, PADFA prohibits certain sales of personally identifiable sensitive data to foreign adversary countries or any entities controlled by a foreign adversary country. These warning letters emphasize the broad scope of data that PADFA covers.

PADFA has emerged as a high-priority enforcement issue for the FTC, as a law at the intersection of privacy concerns about the transfer of sensitive data and broader national security concerns. As we have noted recently, regulators and enforcers are increasingly using consumer protection and privacy laws to address national security and foreign policy goals. With potential penalties up to $53,088 per violation, domestic companies that transfer third-party personal data abroad should review their PADFA compliance.

What PADFA Requires and Who It Impacts

PADFA broadly prohibits data brokers from selling, licensing, transferring, or otherwise providing access to "personally identifiable sensitive data" of U.S. individuals to foreign adversary countries or to any entity controlled by those countries. The law defines a data broker as any company that "for valuable consideration sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals," subject to a few exemptions. PADFA's definition of sensitive data is broad, with

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Ian L. Barlow
Of Counsel
202.719.4994
ibarlow@wiley.law

Practice Areas

Advertising Technology (AdTech) Data Privacy and Consumer Protection

FTC and Consumer Protection

Privacy, Cyber & Data Governance

17 categories of information including data often deemed sensitive under privacy laws, such as government-issued identifiers like Social Security or driver's license numbers, health and financial information, and precise geolocation data. But it also includes any information about a minor and "[i]nformation that reveals the status of an individual as a member of the Armed Forces." Foreign adversary countries include China, Iran, North Korea, and Russia.

The Warning Letters Address Transfer of Data Identifying Military Personnel

The FTC did not identify the specific warning letter recipients, but it released a template as an example. The template letter explains PADFA's basic scope and requirements and does not allege specific violations of the law. But it does state that "[w]e have identified instances in which your company offers or has offered solutions and insights involving the status of an individual as a member of the Armed Forces. Such information is subject to PADFAA's requirements."

The warning letters also urge the recipients to "conduct a comprehensive review of [their] practices and immediately bring [those] acts and practices into compliance" and remind them of the steep civil penalties the FTC may obtain under PADFA. The warning letters are signed by the director of the FTC's Bureau of Consumer Protection, and they identify staff attorneys in that Bureau's privacy enforcement division as contacts for any follow-up questions, indicating engagement on this issue from multiple levels of agency staff.

Key Tips for Companies that Transfer Third-Party Personal Data Abroad

1. *Perform PADFA-specific compliance:*
    - Keep in mind that the definition of a data broker is different under PADFA than under regulations like the U.S. Department of Justice's Data Security Program;
    - Carefully assess whether data is sensitive under PADFA; and
    - Perform appropriate diligence to understand ownership and control of downstream recipients, in light of PADFA's specific thresholds for determining foreign control.
2. *Review and Adjust Data Sharing Practices:*
    - Screen for PADFA-covered sensitive data against lists of prohibited recipients.
    - Ensure contracts and policies reflect PADFA requirements.
3. *Document Compliance Efforts:*
    - Maintain records of risk assessments, compliance policies, training efforts, and remedial actions taken.
    - Always document current compliance. Even if prior policies differed, evidence of current compliance can influence FTC investigative decisions.
    - If your company receives an inquiry from the FTC, consider these tips for responding.