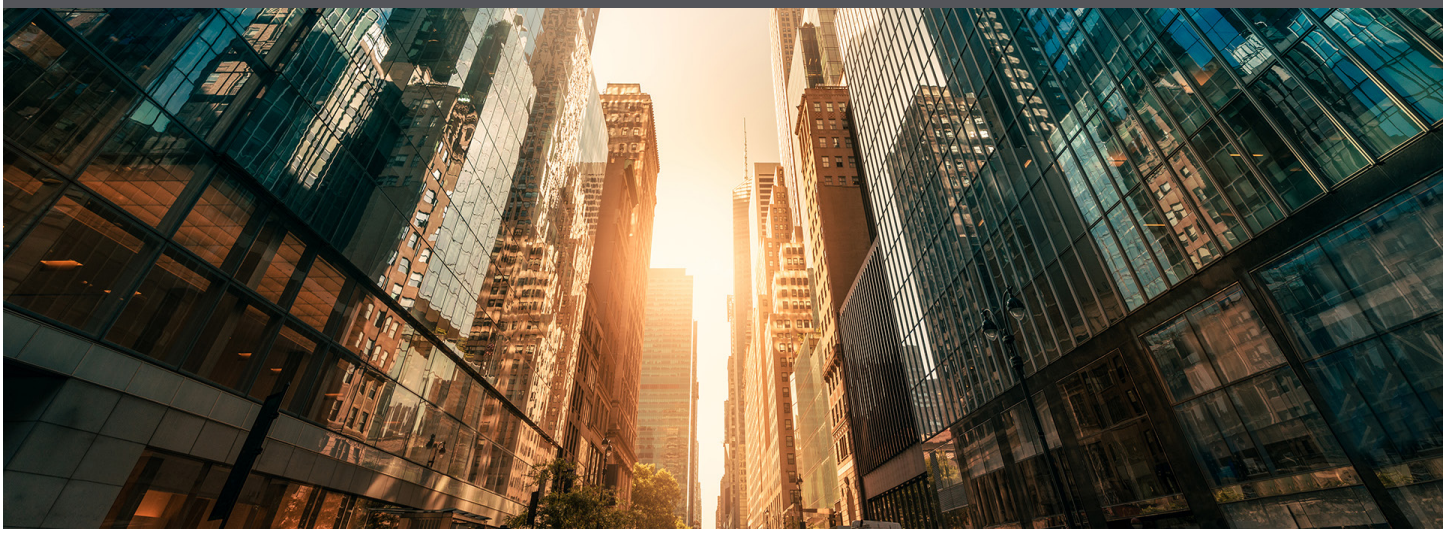
BLANKROME

International Trade



MAY 16, 2024

President Biden Signs into Law Ten-Year Statute of Limitations for Sanctions Violations and Other National Security Measures

President Biden last month signed into law H.R. 815 ("National Security Supplemental" or "NSS"). The NSS—a package of national security and foreign aid appropriations, including for efforts in Israel, Ukraine, and the Indo-Pacific—includes various provisions impacting U.S. national security regulations. Our alert focuses on three particularly notable aspects of the NSS that:

1. Double the statute of limitations for civil and criminal sanctions violations from five to 10 years;
2. Expand efforts to secure American data from use by foreign adversaries; and
3. Authorize the seizure of certain Russian assets "for the purpose of providing assistance to Ukraine."

THREE HIGHLIGHTS

1. Doubling the Statute of Limitations for Sanctions Violations

Division E of the NSS, the Fentanyl Eradication and Narcotics Deterrence Off Fentanyl or "FEND Off Fentanyl Act," while primarily addressing fentanyl trafficking, separately amended the International Economic Emergency Powers Act ("IEEPA") and the Trading with the Enemy Act ("TWEA") to double the statute of limitations—from five to 10 years—for the civil and criminal enforcement of sanctions violations.

Notably, IEEPA and TWEA provide the foundation for the majority of U.S. sanctions administered by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC"). In doubling the statute of limitations for violations under IEEPA and TWEA, Congress signals its intent for the United States to pursue a more aggressive approach toward sanctions enforcement.

While the FEND Off Fentanyl Act does not require OFAC to expand its recordkeeping requirements to keep pace with the amendments to IEEPA and TWEA (persons are currently required to keep a full and accurate record of transactions for at least five years), it seems likely that OFAC will increase the relevant recordkeeping requirement to 10 years and issue guidance concerning the revised statute of limitations.

Importantly, the FEND Off Fentanyl Act does not extend the five-year statute of limitations for violations of the Export Administration Regulations ("EAR")

(although a few provisions in the EAR may be affected by the doubling of the IEEPA penalties) or the International Traffic in Arms Regulations ("ITAR"), which are promulgated under the Export Control Reform Act and the Arms Export Control Act, respectively. However, it is possible that Congress could seek to expand the statute of limitations for EAR and ITAR violations in the future.

The 10-year statute of limitations took immediate effect as of April 24, 2024. The statute is silent as to how the doubling of the statute of limitations might apply to acts committed before the effective date. Standard principles of constitutional law suggest that the new limitations period could apply to any criminal act committed *within* the existing limitations period as of April 24, 2024 (that is, back to April 25, 2019), but likely could not apply to criminal acts committed before that date. The situation is not as clear with respect to imposition of civil penalties.

2. Securing American Data from Foreign Adversaries

The NSS includes new laws concerning foreign adversary access to U.S. personal data: the Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACAA") and the Protecting Americans' Data from Foreign Adversaries Act ("PADFAA") (Divisions H and I of the NSS).

PAFACAA

PAFACAA prohibits Internet hosting services and app stores in the United States from supporting certain applications identified by the President as "controlled" by a foreign adversary country (defined as China, Russia, North Korea, and Iran) and as presenting a threat to national security. Specifically, PAFACAA applies to applications with over one million monthly active users that allow the sharing and viewing of user-generated content. Notably, the law does not apply to companies "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews" via a website or application.

Once an application is determined by the President to be a "foreign adversary controlled application" that presents a significant threat to U.S. national security, owners of the application have 270 days to divest their interest in order to permit the application's continued availability in the United States. If the app undergoes such a divestiture and no longer is considered to be "foreign adversary controlled," then the prohibitions under PAFACAA regarding support for the application cease to be applicable.

Notably, the bill explicitly targets TikTok and its parent company, ByteDance, Ltd., which has 270 days from the date of PAFACAA's enactment (i.e., until January 19, 2025) to divest itself of TikTok in the United States.

Despite Congressional focus on TikTok, PAFACAA potentially applies to any social media application with more than one million active users that is "controlled by a foreign adversary" and determined by the President to be "a significant threat to U.S. national security." To determine that an application is a national security threat, the President is required to issue a public notice to that effect and report to Congress explaining the basis of his judgment. Thus, the President can ban any social media application that is "controlled" by an adversary country.

"Controlled by a foreign adversary" means that such company is: (a) a non-U.S. entity incorporated in or with a principal place of business in a foreign adversary country; (b) an entity which is at least 20 percent owned (directly or indirectly) by a foreign entity that falls within Category (a); or (c) an entity subject to the direction or control of a foreign entity described in Categories (a) or (b).

On May 7, 2024, TikTok and its parent company, ByteDance, filed suit in the U.S. Court of Appeals for the District of Columbia Circuit in accordance with the judicial review provisions in PAFACAA, challenging the law on First Amendment grounds.

PADFAA

PADFAA prohibits "data brokers" from selling, licensing, renting, trading, transferring, releasing, disclosing, providing access to, or otherwise making available personally identifiable sensitive data of a U.S. individual to any foreign adversary or any entity controlled by a foreign adversary. A "data broker" is defined as:

"an entity 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 to another entity that is not acting as a service provider."

The law mainly focuses on the protection of "personally identifiable sensitive data" from access by a foreign adversary country (or an entity controlled by one).

PADFAA includes in its definition of "sensitive data" 16 separate categories, including:

- A government issued identifier (e.g., SSN, passport number, driver's license number);
- Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual;
- A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual;
- Biometric information;
- Genetic information;
- Precise geolocation information;
- Private communications;
- Account or device log-in credentials;
- Information identifying the sexual behavior of an individual;
- Calendar information;
- Media showing the naked or undergarment-clad private area of an individual;
- Information revealing the video content requested or selected by an individual;
- Information about an individual under the age of 17;
- An individual's race, color, ethnicity, or religion;
- Information identifying an individual's online activities over time and across websites; and
- Information revealing the status of an individual as a member of the Armed Forces.

Sensitive data is considered "personally identifiable" if it "identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linked to an individual." Violations of PADFAA will be treated as violations of rules regarding unfair or deceptive acts under the Federal Trade Commission Act.

Notably, PADFAA potentially overlaps with Executive Order 14117, which aims to prohibit or restrict access to bulk sensitive U.S. personal data or government-related data by certain countries. Executive Order 14117 delegated authority to the U.S. Department of Justice's ("DOJ") National Security Division, and the DOJ recently published a corresponding Advance Notice of Proposed Rulemaking ("ANPRM").

PADFAA goes into effect on June 23, 2024

3. Authorizing the Seizure of Certain Russian Assets for Aid to Ukraine

Division F of the NSS, the Rebuilding Economic Prosperity and Opportunity for Ukrainians Act, or "REPO for Ukrainians Act," permits the President to "seize, confiscate, transfer, or vest any Russian state sovereign assets . . . including any interest or interests in such assets" to transfer those funds to a "Ukraine Support Fund" to be created under the new law.

To do so, the President must satisfy a certification framework, which requires that (1) such actions are "in the national interest," (2) the President has "meaningfully coordinated with G7 leaders to take such multilateral action," and (3) either the President has received a request from a certain "properly constituted international mechanism" or Russia has not ceased its aggression against Ukraine or has ceased its aggression but is not working to provide Ukraine full compensation.

The new Ukraine Support Fund is intended to be comprised of any frozen Russian sovereign funds that are seized pursuant to the REPO for Ukrainians Act. Such funds are to be used solely for providing assistance to Ukraine for damage "resulting from the unlawful invasion by the Russian Federation."

Given current estimates that only 1 to 2 percent of the $300 billion in frozen Russian sovereign assets are subject to U.S. jurisdiction (with the remainder reportedly held in Europe), the law also emphasizes multilateral cooperation among U.S. allies. Specifically, it requires the President to take appropriate action to coordinate with allies, including seeking to establish an international mechanism, as mentioned above, which may include an international fund called the "Ukraine Compensation Fund."

KEY TAKEAWAYS

Expanded statute of limitations:

- The expanded statute of limitations could significantly impact how companies approach internal investigations, voluntary disclosures, and mergers and acquisitions due diligence.
- It is unclear whether companies may be held civilly liable for sanctions violations which had previously been time-barred under the five-year statute of limitations.
- Companies should consider strengthening compliance programs to expand record retention requirements to 10 years, particularly in the event that OFAC issues updated recordkeeping requirements.

Securing personal data:

- Both PAFACAA and PADFAA represent significant efforts to address emerging threats to national security and personal data privacy posed by foreign adversaries in the digital age.
- PAFACAA empowers the President to impose restrictions on certain applications "controlled" by foreign adversaries, apparently including those maintained by U.S. companies that have already cleared foreign investment screening by the Committee on Foreign Investment in the United States.
- PADFAA appears to overlap with EO 14117, and it remains to be seen how the Biden Administration will implement the relevant restrictions.

Seizure of Russian assets:

- The REPO for Ukrainians Act establishes a framework for the President to confiscate sovereign Russian assets for use in Ukraine recovery, which could be of interest to parties in Ukraine seeking compensation for damages sustained as a result of Russia's invasion.

For more information or assistance, contact Anthony Rapa, Alan G. Kashdan, Brendan S. Saslow, Patrick F. Collins, Rachel D. Evans, or another member of Blank Rome's International Trade group.

Anthony Rapa
202.420.2683 | anthony.rapa@blankrome.com

Alan G. Kashdan
202.420.2658 | alan.kashdan@blankrome.com

Brendan S. Saslow
202.420.2287 | brendan.saslow@blankrome.com

Patrick F. Collins
202.420.2594 | patrick.collins@blankrome.com

Rachel D. Evans
202.420.2327 | rachel.evans@blankrome.com