Lowenstein Sandler

Trade Matters

Lowenstein Sandler's Global Trade & Policy Newsletter

June 2021

Share:

1. Recent Enforcement: Even Companies That Invest in Compliance Pay Penalties

Since our April enforcement roundup, the Office of Foreign Assets Control (OFAC) and the Bureau of Industry and Security (BIS) in the Department of Commerce have issued several important penalty announcements. These enforcement actions demonstrate that even multinational companies that invest in compliance can run into problems without a continued commitment to monitoring and updating their programs.

- Global software company SAP SE paid a total of $8 million in a combined global resolution with the Department of Justice (DOJ), Commerce, and Treasury for illegal exports, and it also disgorged $5.14 million in profits. Between December 2009 and September 2019, the company exported its software, upgrades, and patches more than 20,000 times to end users in sanctioned countries, including Iran, without a license. As part of the settlement, SAP must perform three internal audits of its export compliance program over the next three years. This is in addition to the $27 million SAP reportedly spent to enhance its existing compliance program. This is the first case where the DOJ's National Security Division applied its new Export Control and Sanctions Enforcement Policy for Business Organizations, crediting SAP with voluntary disclosure, cooperation, and remediation.
- The State Department fined U.S. aerospace and technology company Honeywell International Inc. $13 million for illegally exporting technical data to several countries, including China. Between 2011 and 2018, the company committed 34 violations of the International Traffic in Arms Regulations (ITAR) and the Arms Export Control Act, sending drawings of parts for military-related items, including ITAR-controlled items like engines of military jets and bombers. Honeywell discovered that

Contact Us

for more information about any matters in this newsletter:

Doreen M. Edelman
Partner
Chair, Global Trade & Policy
202.753.3808
dedelman@lowenstein.com

Laura Fraedrich
Senior Counsel
202.753.3659
lfraedrich@lowenstein.com

Abbey E. Baker
Counsel
202.753.3806
abaker@lowenstein.com

Andrew Bisbas
Counsel
202.753.3807
abisbas@lowenstein.com

Christian C. Contardo
Associate
202.753.3804
ccontardo@lowenstein.com

Megan C. Bodie

some of the employees were not following the manufacturer's own compliance plan, which highlighted the importance of regular reviews of and training on compliance policies.

- MoneyGram Payment Systems Inc., a global payments company, has agreed to remit $34,328.78 to settle its liability for 359 violations of several sanctions programs. Between March 2013 and April 2016, MoneyGram conducted money transfers to the DOJ's Federal Bureau of Prisons (BOP) to allow inmates to send and receive funds into and out of their personal commissary accounts. MoneyGram did not screen these inmates' names against OFAC's Specially Designated Nationals and Blocked Persons (SDN) List despite knowing that some of the inmates could be on the SDN List; it believed that the screening was not required under the BOP program. Later, the company did implement a screening process, but it nonetheless continued to process transactions on behalf of blocked persons in federal prisons due to other screening, technology, and fuzzy logic failures as well as limited instances of human error. Money services businesses that are processing transactions for individuals worldwide should understand their obligations under U.S. sanctions programs and should mitigate the risks associated with those services by properly implementing and maintaining a sanctions screening process.

2. Commerce Issues Subpoenas Under New Technology Authority

In March and April, the Department of Commerce issued subpoenas to several Chinese companies under a new rule that gives the Secretary of Commerce the power to ban or restrict certain transactions that touch the "Information and Communications Technology and Services [ICTS] Supply Chain." Commerce can block or require mitigation steps for transactions involving technologies that have been "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" and that pose an undue or unacceptable risk to the national security of the United States. The "foreign adversaries" include China, Russia, Iran, North Korea, Cuba, and Venezuela. The types of ICTS transactions include the 16 critical infrastructure sectors; connectivity; sensitive personal data; sensors, routers, and drones; communications and apps; and artificial intelligence and machine learning. Commerce is still determining what the licensing or preclearance process will look like; the Committee on Foreign Investment in the United States process is a likely model. This new process highlights the need to know where your technology originates.

3. Cybersecurity Executive Order (E.O.) Requires Security Standards for Government Tech Suppliers

Executive Order 14028, signed on May 12, seeks to combat digital threats to U.S. networks and infrastructure. The E.O. requires baseline security standards for software developed for or licensed to the government; software developers must maintain greater visibility into their software and make the security data publicly available. In addition, the E.O. establishes a pilot program similar to the Energy Star program to label software that is developed securely. And while the directives in the E.O. only apply to U.S. federal

Administrative Coordinator
202.753.3809
mbodie@lowenstein.com

Subscribe–and stay in the know!

If you would like to update your mailing preferences for Lowenstein Sandler communications, please click here.

MANAGE MY PREFERENCES

departments and agencies and their technology suppliers, we expect that they will also be adopted by the broader public and become standard practice.

Trade tip of the month: Global online businesses must understand and review internet protocol (IP) data to mitigate economic sanctions risk. In its December 2020 settlement with BitGo Inc., OFAC determined that BitGo had reason to know that users were located in sanctioned countries based on IP data it had obtained but failed to review. OFAC previously cited other companies, including Standard Chartered Bank, for failure to implement IP geo-blocking.

Additional Resources

- **Article:** "CFIUS doesn't mean Chinese companies can't invest in the US"
  May 5, 2021
  TechNode
  Doreen M. Edelman, Laura Fraedrich, and Christian C. Contardo
- **Article:** "How An Effective Trade Compliance Program Saves Money"
  October 16, 2020
  Industry Today
  Doreen M. Edelman and Andrew Bisbas
- **Article:** "Compliance Program 'Must Haves' for Doing Business Abroad"
  July 30, 2020
  Lowenstein Sandler LLP
  Doreen M. Edelman

Follow us on:

lowenstein.com

NEW YORK PALO ALTO NEW JERSEY UTAH WASHINGTON, D.C.