Foreign Investment & Trade Alert

Weil

September 12, 2024

CFIUS Is Locked and Loaded, but What Lies Ahead for CFIUS Enforcement Activity?

By Shawn Cooley, Nathan Cunningham and Christina Carone

The Committee on Foreign Investment in the United States ("CFIUS" or "the Committee") has published new details and guidance on its enforcement activities on the Department of Treasury's website, including, for the first time, a comprehensive list of civil monetary penalties it has imposed. CFIUS also provides insight on factors informing issuance of Determination of Noncompliance Transmittal ("DONT") Letters, which CFIUS sends to parties that CFIUS has determined violated CFIUS' regulations or a national security risk-mitigation agreement.

Key Highlights:

- CFIUS has issued civil monetary penalties ranging from $100,000 to $60,000,000.
- Of the eight penalties CFIUS has disclosed, seven were issued because of violations of material terms of a national security risk-mitigation agreement or an interim order and one was issued because of forged documents submitted to CFIUS and multiple material misstatements made by the foreign buyer.
- CFIUS issued two separate penalties relating to failure to adequately restrict access to sensitive data and failure to divest foreign ownership interests in a timely fashion, each as required by the applicable mitigation agreement or interim order.
- CFIUS is highly focused on identifying any missed mandatory filing requirements, which will remain a key enforcement priority.
- CFIUS is serious about enforcement as evidenced by its increased enforcement staffing, dedicated resources, and use of penalties and DONT Letters.

Enforcement Actions That Resulted in Penalties

CFIUS recently provided new insight into its new enforcement era by publishing on its website a list of eight enforcement actions involving monetary penalties pursuant to Section 721(h) of the Defense Production Act of 1950. CFIUS took into account the objectives of enforcement and national security, among other factors, when assessing the following penalties:

Notice of Penalty Year	Party Penalized	Reason(s) for the Penalty	Penalty Amount (USD)
2024	T-Mobile US, Inc.	In 2018, T-Mobile (ultimately owned by a German entity) entered into a National Security Agreement ("NSA") with CFIUS in connection with the T-Mobile and Sprint merger. T-Mobile violated a material provision of the NSA because it failed to prevent unauthorized access to certain sensitive data and failed to timely report certain incidents of unauthorized access to CFIUS. CFIUS did not otherwise disclose any applicable aggravating or mitigating factors.	$60 Million
2024	Unknown	The company's majority shareholders removed all of the company's independent directors, causing the Security Director position to be vacant and the board of directors' government security committee to be nonoperational. This constituted a breach of the NSA because the company did not ensure that the compliance oversight responsibilities assigned to the Security Director and to the government security committee under the NSA were or could be performed. CFIUS did not otherwise disclose any applicable aggravating or mitigating factors.	$8.5 Million
2024	Unknown	The foreign acquirer submitted a joint voluntary notice ("JVN") and supplemental information that contained five material misstatements, including forged documentation and signatures. In addition, the foreign acquirer made material misstatements regarding the source of funding for the transaction and related agreements during CFIUS' review. CFIUS rejected the filing due to the misstatements, and the parties abandoned the transaction. CFIUS did not otherwise disclose any applicable aggravating or mitigating factors.	$1.25 Million
2023	Unknown	The U.S. business failed to maintain a statement on its website regarding its foreign ownership, as required by the Letter of Assurance ("LOA"). Since the customers of the U.S. business may have lacked knowledge of its foreign ownership, data and technology potentially could have been exposed to the foreign ownership, which could have caused the customers to violate aspects of U.S. government contracts. CFIUS considered the following aggravating factors: the duration of the violations, managerial involvement in the violations, failure to self-disclose the violations, and the U.S. business's lack of compliance procedures and training. CFIUS considered the U.S. business's cooperation with the Committee during its investigation a mitigating factor.	$990,000

2023	Unknown	The transaction parties did not divest the foreign acquirer's interest in the U.S. business by the date specified in the NSA. CFIUS considered the following aggravating factors: repeated violations of other NSA provisions, prolonged failure to make serious efforts to divest, and the transaction party's failure to provide prompt notice to CFIUS of its failure to meet the divestment deadline. As mitigating factors, CFIUS considered difficult market conditions during the COVID pandemic, among others.	$200,000
2023	Unknown	Here again, the transaction parties failed to divest the foreign acquirer's interest in the U.S. business by the date required in the NSA. CFIUS considered the following aggravating factors: repeated violations of other NSA provisions, prolonged failure to make serious efforts to divest, and failure to timely notify CFIUS that it would be unable to meet the divestment deadline. CFIUS considered the transaction party's small size and lack of sophistication, and the particularly difficult market conditions during the COVID pandemic as mitigating factors.	$100,000
2019	Unknown	A transaction party violated a CFIUS interim order because it did not restrict and adequately monitor access to protected data. CFIUS did not otherwise disclose any applicable aggravating or mitigating factors.	$750,000
2018	Unknown	A transaction party failed to establish security policies and to provide adequate reports to CFIUS, each as required by the applicable NSA. CFIUS did not otherwise disclose any attendant aggravating or mitigating factors.	$100,000

These penalties exist within the context of CFIUS' proposed rule to increase the maximum penalty per violation, in certain instances, to $5,000,000 from $250,000.[i] CFIUS expressly stated on its website that the $1.25 million penalty, imposed in 2024 as a result of multiple material misstatements (including forged documents and signatures) made during the review process, was the maximum penalty permitted under CFIUS' regulations. If CFIUS implements this proposed rule, the maximum penalty in a similar circumstance (*i.e.*, with five material misstatements) would be $25,000,000.

Determination of Noncompliance Transmittal ("DONT") Letters

CFIUS also provided significant new insight via its website regarding its use of DONT Letters, with which CFIUS notifies parties of its determination that they have violated CFIUS' regulations or a mitigation agreement. A DONT Letter itself does not impose a penalty, but could be a pre-cursor to CFIUS' issuing a penalty. Per CFIUS' guidance, a DONT Letter will either inform the parties that CFIUS has elected not to issue a penalty or that CFIUS requires additional information to determine whether a penalty is warranted. Even if the DONT Letter does not result in a penalty, CFIUS at a later date could consider the existence of a violation identified in a DONT Letter as an aggravating factor in a subsequent enforcement proceeding.

Generally, CFIUS has issued a DONT Letter without progressing to monetary penalties where the violation was:

- A first-time violation for the party,
- Inadvertent, and/or
- Limited in scope such that it did not harm U.S. national security interests and had little potential to do so.

When determining whether to issue a DONT Letter, CFIUS also considers the extent to which the parties:

- Made a voluntary self-disclosure,
- Remediated the violation(s),
- Cooperated with CFIUS' enforcement proceeding,
- Operate an otherwise strong compliance program, and/or
- Were subject to difficult extrinsic circumstances.

While CFIUS may determine that a violation merits a penalty even where some or all of these factors exist, CFIUS has provided examples of cases where CFIUS merely issued a DONT Letter and did not progress to issuing a penalty:

- Failing to timely submit a mandatory declaration when it was a first-time offense and there was no resulting harm to national security and little potential for such harm.
- Failing to utilize a segregated network for certain protected information, as required by a CFIUS mitigation agreement.
- Transferring assets to a company controlled by certain foreign persons in violation of a CFIUS order.
- Failing to prevent unauthorized access to intellectual property restricted by CFIUS mitigation.

This guidance provided by CFIUS is a useful framework for understanding what can be an opaque enforcement process. Each circumstance, however, is unique and robust consideration of CFIUS' regulations and strict compliance with any applicable mitigation terms remains the surest path to avoiding CFIUS' increasingly aggressive enforcement posture.

Is a $60m Fine Reasonable Under the Circumstances?

As referenced above, CFIUS identified a national security risk resulting from the merger of Sprint Corporation ("Sprint") and T-Mobile US ("T-Mobile"), resulting in CFIUS' requiring the parties to execute a NSA as a condition for obtaining CFIUS clearance in 2018. Based on publicly available information, Deutsche Telekom, a German telecommunications company, owns a majority interest in T-Mobile. Additionally, as mentioned above, CFIUS considered it appropriate to issue a $60,000,000 penalty to T-Mobile because it did not prevent access to certain sensitive data. Deutsche Telekom is domiciled in Germany, which is part of the European Union ("EU") and an ally of the United States. Assuming for the moment that totality of the circumstances supports CFIUS' findings regarding both the violations and the penalty, it may be worth understanding in the first instance why CFIUS required a NSA from a well-known EU entity like Deutsche Telecom.

For context, Sprint was subject to a preexisting NSA related to a 2013 transaction between Sprint and SoftBank prior to T-Mobile acquiring Sprint in 2020.[ii] In that NSA, Sprint and SoftBank agreed to several conditions, including a requirement to rip and replace all Huawei equipment already deployed on its U.S. network and giving the Departments of Defense, Homeland Security, and Justice the power to review and veto new equipment purchases in specific circumstances.[iii] This very well could have been the most costly

mitigation ever required by CFIUS. CFIUS' continued concern with Sprint in 2018 presumably emanated from Deutsche Telecom's then use of Huawei equipment outside of the United States.[iv]

As discussed above, CFIUS stated that between August 2020 and June 2021 T-Mobile failed to take appropriate action to prevent unauthorized access to certain sensitive data and failed to report certain incidents in a timely manner, in violation of its NSA and delaying the Committee's investigation, respectively.[v] T-Mobile stated the incidents were related to unauthorized access of information shared in response to law enforcement requests and that these incidents occurred due to technical issues the company experienced during the post-merger integration with Sprint. Further, T-Mobile also said that the information did not leave the U.S. law enforcement community.[vi] Given this, it is reasonable to question how such unauthorized access could have resulted in any material "harm to the national security equities of the United States."[vii] And even if it did, how is a $60,000,000 fine proportionate to any purported harm, especially if such access occurred because of what appears to be mere integration growing pains generally common with any merger of two large companies?

Should CFIUS Bifurcate the Enforcement of Mitigation Measures from the Enforcement of its Regulations?

Of the eight penalties imposed by CFIUS in its 50-year history, seven resulted principally from violation of material terms of mitigation measures, such as NSAs or interim orders, and one resulted principally from material misstatements made during the CFIUS review period. CFIUS' regulations, Enforcement and Penalty Guidelines, and enforcement webpage each address in the same manner violations of NSA provisions and violations of other aspects of CFIUS' regulations. Presuming CFIUS' recent significant uptick in enforcement activity presages continued robust enforcement actions, could CFIUS find it beneficial to treat NSA-related violations differently than other violations? Could enforcing pursuant to the same guidelines violations of material NSA terms, which are inherently contractual in nature, and other violations of CFIUS' regulations, which principally exist as a result of regulatory fiat, result in undesirable inconsistencies or incongruities?

For instance, a technical, but material violation of a NSA provision from issues attendant to post-transaction integration and initial implementation of the NSA could, in a CFIUS monitoring agency's ("CMA")[viii] view, warrant no monetary penalty. In contrast, CFIUS could view parties' failure to make a mandatory filing as warranting a significant monetary penalty, even if similar aggravating and mitigating factors exist in the two circumstances. Such a disconnect could result from a divergence of approach among the CMAs vis-à-vis the other CFIUS member agencies since the CMAs could be more inclined to give greater weight to mitigating factors to nurture an on-going cooperative and trust-based relationship. In the context of noncompliance with CFIUS' regulations, however, CFIUS could be less inclined to weigh such mitigating factors in an effort to maximize the potential deterrent effect.

Historically, CMAs have prioritized open communication with NSA parties and prompt rectification of any NSA violation by recognizing existing mitigating factors, such as a lack of experience with CFIUS concepts and regulations combined with good faith and prompt remediation. This approach recognized that a heavy-handed adversarial approach could deter parties from sharing any NSA implementation or other compliance difficulties out of fear of exposing themselves to penalties rather than opening a dialogue to facilitate sustainable, long-term compliance in the face of an ongoing necessity to account for an identified national security risk. The same considerations do not apply in the context of violations of CFIUS' regulations that are unrelated to mitigation measures. In that sense, aggressive enforcement of non-mitigation aspects of CFIUS' regulations (such as a failure to submit a mandatory filing or provision of a material misstatement) would not necessarily result in the same disadvantages or inefficacies that could follow aggressive assessment of penalties for non-egregious violations of material NSA terms.

Conclusion:

CFIUS' website update confirms it remains committed to expanding all enforcement activity. CFIUS will continue to look aggressively for instances of non-compliance with its regulations and mitigation measures, but to be most effective CFIUS should continue to ensure that its enforcement actions also demonstrate restraint and proportionality where appropriate in as transparent of a process as possible. It is now more important than ever for transaction parties to conduct and document thorough CFIUS due diligence when pursuing a transaction implicating CFIUS' jurisdiction, especially when the presence of critical technologies, critical infrastructure, or sensitive personal data could result in a mandatory filing obligation. Further, it is imperative for transaction parties to fully comprehend the obligations and burdens implicationed by complex mitigation terms and the path to timely implement and maintain ongoing compliance with them.

* * *

If you have questions concerning the contents of this alert, or would like more information, please speak to your regular contact at Weil or to the authors:

Authors

Shawn Cooley (D.C.)	View Bio	shawn.cooley@weil.com	+1 202 682 7103
Nathan Cunningham (D.C.)	View Bio	nathan.cunningham@weil.com	+1 202 682 7156

[i] *See* Amendments to Penalty Provisions, Provision of Information, Negotiation of Mitigation Agreements, and Other Procedures Pertaining to Certain Investments in the United States by Foreign Persons and Certain Transactions by Foreign Persons Involving Real Estate in the United States, 89 Fed. Reg. 26107 (Dept. Treasury, Apr. 15, 2024). Treasury has not yet implemented this proposed rule.

[ii] *See* https://www.reuters.com/article/technology/sprint-softbank-agree-to-u-s-national-security-deal-idUSBRE94S0IG/.

[iii] *See* id.

[iv] *See* https://www.reuters.com/article/world/exclusive-t-mobile-sprint-see-huawei-shun-clinching-us-deal-sources-idUSKBN1OD2IA/.

[v] *See* https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement.

[vi] *See* https://www.wsj.com/articles/t-mobile-fined-60-million-to-settle-alleged-national-security-violations-36b22b05.

[vii] *See* https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement.

[viii] As the name suggests, an agency is a CFIUS monitoring agency only in the context of CFIUS mitigation. The designation of "CMA" is not applicable outside the mitigation context (*i.e.*, it is not applicable in a context limited to a violation of other aspects of CFIUS' regulations, such as the failure to submit a mandatory notification or the provision of material misstatements in the context of a CFIUS review).