Proskauer

National Security Reviews Continue Apace: CFIUS Orders Unwinding of Transaction Involving Hotel Guest Data Firm

March 24, 2020

Following the February 13, 2020 effective date of the U.S. Department of Treasury's final regulations (the "Final Rules") implementing the majority of the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"), foreign investment in the United States is facing continued close scrutiny and attention with the Committee on Foreign Investment in the United States ("CFIUS") making headlines ordering the unwinding of another completed transaction.

On March 6, 2020, at CFIUS' recommendation, President Trump issued an executive order requiring Chinese company Beijing Shiji Information Technology Co., Ltd. ("Shiji") to divest all interest it holds in the assets and operations of StayNTouch.

StayNTouch is a U.S. hotel-guest data firm that offers "software as a service" for a mobile property management system (PMS). Shiji acquired StayNTouch in 2018. Companies in the hospitality industry use PMS systems to optimize their services, with the aim of increasing their level of services and revenues while reducing costs. One way the StayNTouch (and other PMS systems) achieves this is by personalizing services, which is based on hotels' (or other service providers') ability to manage and collect information from their guests, including names, phone numbers, credit card numbers, and the dates and locations of customers' hotel stays.

Nearly all hotel management companies use PMS and other similar systems to manage hotel operations. Most have invested significant amounts of money in developing and upgrading their PMS systems over the past few years. Many have also invested heavily in their loyalty programs, which also collect similar information from guests and customers. We have indicated before[1] that the new regulations could apply to such systems; and based on the StayNTouch ruling, any company in the industry (hotels, restaurants, tour guides, airlines, etc.) that has foreign owners and that is developing or using a PMS or loyalty system (or using a system operated or licensed from another company that has foreign owners) will need to assess how to address this issue.

In the executive order, Trump cited "credible evidence" that Shiji, through its acquisition of interest in StayNTouch, "might take action that threatens to impair the national security of the United States." Accordingly, Shiji must immediately put controls in place to prevent access to StayNTouch's data until the divestiture is completed, and Shiji was given 120 days to fully divest its interest in StayNTouch. CFIUS is "authorized to implement measures it deems necessary and appropriate to verify compliance," including physical access to "all premises and facilities of StayNTouch located in the United States," to inspect and copy any books, ledgers, accounts, correspondence, memoranda, information systems, and data, and to interview any employees of Shiji or StayNTouch.

This is not the first transaction upended over CFIUS' newfound concerns under FIRRMA relating to sensitive personal data of U.S. citizens. In 2019, CFIUS ordered two divestitures of investments by Chinese firms in U.S. companies that collect such data: Beijing Kunlun Tech Co.'s investment in dating platform Grindr; and iCarbonX's investment in health tech startup PatientsLikeMe. Neither transaction was subject to the mandatory pre-closing CFIUS filing requirements, and neither went through the voluntary pre-closing review process.

CFIUS' actions taken on the three transactions make it clear that it views any investment in a company that "maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security" as presenting heightened risk in a post-FIRRMA world. This is especially true for investments originating in countries facing stepped-up U.S. national security efforts. Those investors and others should implement diligence efforts to identify what types of sensitive personal data the target firm collects, and to determine whether it is potentially within the scope of CFIUS review under 31 C.F.R. 800.241[2] (such as geolocation data, for instance, collected for customer marketing or experience programs) or otherwise raises national security concerns. Where the collected data is within scope of, and potentially raises, national security issues, mitigation plans addressing those concerns up-front, such as isolating data and otherwise limiting access, can help streamline the review process and reduce the likelihood of adverse CFIUS action.

CFIUS' increased scrutiny of investment in U.S. critical technologies was also recently tested by German-based Infineon's proposed acquisition of U.S.-based Cypress Semiconductor. According to public sources, the transaction, announced in June 2019, combines leading semiconductor firms under foreign ownership with close ties to Chinese investors. The companies reportedly withdrew and resubmitted their CFIUS paperwork at least once. However, ultimately they were successful in negotiating a mitigation agreement that satisfied CFIUS' national security concerns. The terms of that agreement, while not public, are likely to include requiring protections for and monitoring of Cypress' most sensitive critical technology-related data. The firms released a statement on March 9, 2020 that CFIUS had ended its investigation, and the transaction was permitted to proceed. The take-away message is that the U.S. remains open to foreign investment, even into its most sensitive industries, but that close evaluations and case-by-case assessments are the order of the day. Parties entering into transactions potentially raising national security concerns must make an independent evaluation of the risk profile and transact accordingly. For example, counsel should consider building prophylactic provisions into transaction documents, such as conditions to closing to protect against potentially onerous CFIUS mitigation requirements.

CFIUS Filing Fees

As discussed in our previous alert, the majority of FIRRMA's provisions were implemented in the Final Rules. However, the rule-making process is ongoing, and on March 9, 2020, the Treasury Department published another set of proposed rules (the "Proposed Rules") for one of the few outstanding items under FIRRMA: filing fees. With the implementation of these fees, CFIUS has expressed a desire to "minimize the impact on small businesses" while also recouping the costs required to exercise its expanded jurisdiction under FIRRMA.

Under the Proposed Rules, filing fees range from $750 to $300,000, depending on the value of the transaction, and would apply to long-form voluntary notices for transactions falling under CFIUS' jurisdiction. CFIUS would not begin its investigation until the filing fee is paid. No fees would be imposed for short-form declarations, and transactions valued under $500,000 would be exempt. FIRRMA authorizes CFIUS to impose filing fees up to the lesser of one percent of the value of a transaction or $300,000, adjusted annually for inflation. CFIUS' proposed fee schedule is as follows:

TRANSACTION VALUE	FILING FEE
Less than $500,000	**$0**
Between $500,000 and $5 million	**$750**
Between $5 million and $50 million	**$7,500**
Between $50 million and $250 million	**$75,000**
Between $250 million and $750 million	**$150,000**
Greater than $750 million	**$300,000**

Under the Proposed Rules the value of a transaction includes "the total value of all consideration that has been or will be provided in the context of the transaction by or on behalf of the foreign person … including cash, assets, shares or other ownership interests, debt forgiveness, or services or other in-kind consideration." Where the transaction value is unknown, fair market value as of the date of filing the notice will control. The Proposed Rules also address how CFIUS plans to assess values in joint ventures and transactions completed in multiple phases. Upon filing with CFIUS, parties will be required to explain the methodology they used to calculate transaction value.

While the fee amount will generally be based on the entirety of a transaction, the Proposed Rules exempt certain transactions involving only a limited U.S. presence. If a transaction has a total value of more than $5 million, but the interests or rights acquired in the U.S. business is less than $5 million, the filing fee would be capped at $750. This exception would not apply to covered real estate transactions.

Since the Final Rules allow parties to submit a declaration in lieu of a notice, parties have the option to submit without paying a filing fee. However, CFIUS is not required to reach a conclusion regarding whether a national security risk is present on the basis of a declaration alone. The decision to initially forgo a voluntary notice could ultimately lead to filing one (and paying the required fee) in two scenarios after submission of a declaration: (1) CFIUS requests that the parties submit a full voluntary filing, or (2) CFIUS is unable to make a definitive judgment on national security risk based on the declaration alone. In the second scenario, many parties may choose to file a voluntary notice to compel CFIUS to make a final decision before completion of a deal, rather to than leave the door open for review later down the road.

Parties who do make the decision to file voluntary notices will not be charged an additional fee for withdrawing and refiling their notices, unless there is a material change to the transaction, or CFIUS determines that a material inaccuracy or omission was made in the initial filing. CFIUS will also not issue refunds of filing fees, unless it determines during review that it lacks jurisdiction over a transaction.

CFIUS is accepting comments on the Proposed Rules until April 8, 2020.

* * *

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. Visit our **Coronavirus Resource Center** for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

---

[1] Geolocation data collected using positioning systems, cell phone towers, or Wi-Fi access points, such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device (e.g., location data on customers collected and maintained for customer marketing or customer experience purposes; or for mobile mapping services)

[2] Data that could be used to determine a persons financial distress; data contained in a consumer report (unless limited data is obtained from a consumer reporting agency for purposes described in the Fair Credit Reporting Act); data contained in insurance applications; data that relates to a persons physical, mental or psychological well-being (i.e., health information); non-public electronic communications, including, email messaging, or chat communications between or among users of a U.S business products or services; geolocation data; biometric enrollment data; data concerning U.S. government personnel security clearance; and data in an application for U.S. government security clearance.

Related Professionals

- **John R. Ingrassia**
  Partner
- **Yuval Tal**
  Partner