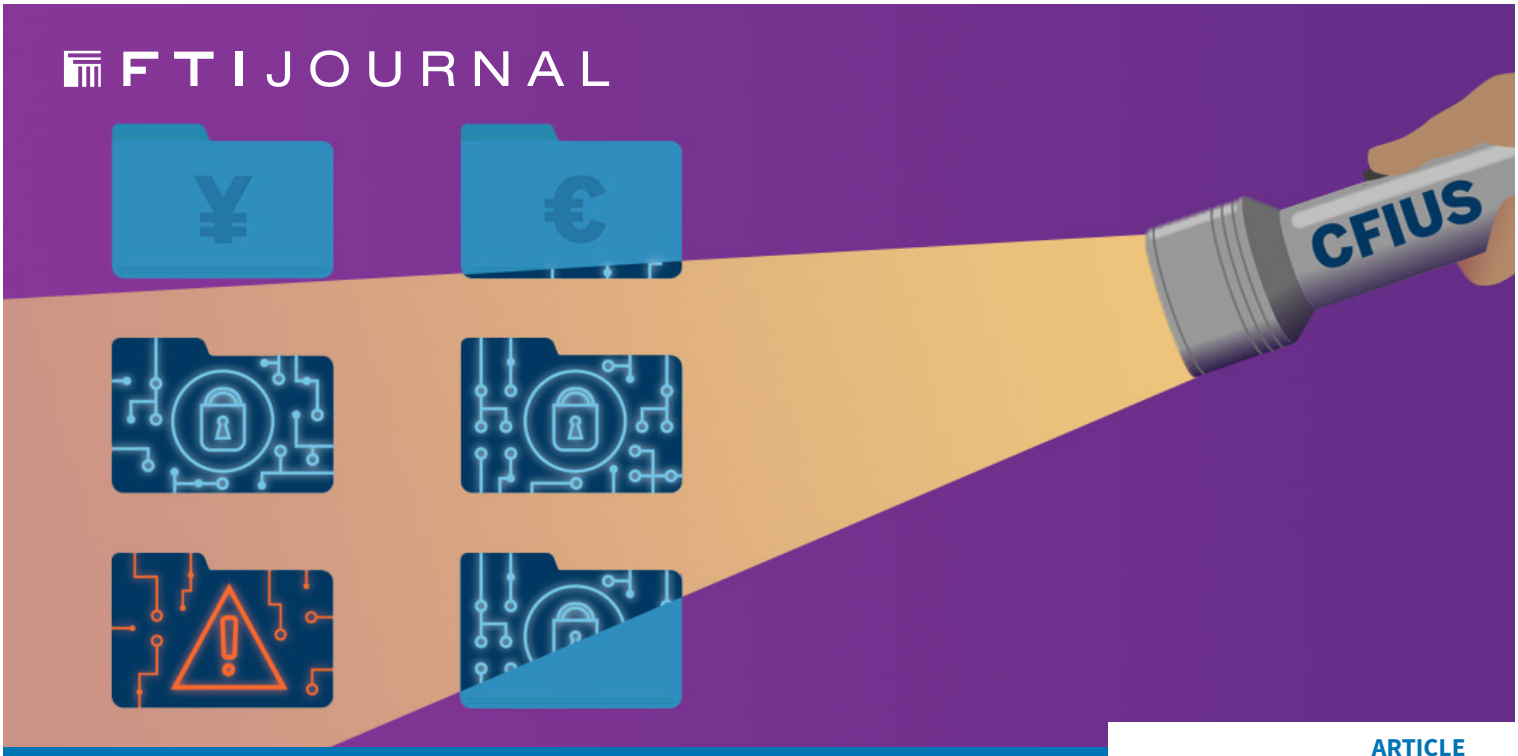
FTI JOURNAL



ARTICLE

CFIUS is Eyeing Your Data. You Should, Too

April 2021

The Feds are aggressively scrutinizing foreign investment in the United States. Whether your agreement is pending or approved, protecting your data and intellectual property is a critical — and often overlooked — element in mitigating deal risk.

It's said that data is the new oil. It's said that data is worth its weight in gold. But there's one thing often left unsaid about this valuable commodity that certain U.S. businesses and foreign investors engaged in an M&A should know: The way each party manages data can raise a red flag with the United States government.

The issue applies to U.S. businesses involved in critical technology (i.e. export controlled technology), infrastructure or sensitive data, and is driven by CFIUS, the Committee on Foreign Investment in the United States. CFIUS has gained significant strength over the past few years, thanks to a sizeable boost in federal funding under the Trump administration. New rules following the passage of the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018 expanded the committee's authority to review and restrict foreign investments on national security grounds.

Accountability is key for deal participants: CFIUS has the power to potentially block a broad array of "covered" transactions (see sidebar) when assessing national security implications. The committee is particularly focused on the way in which each party manages and safeguards intellectual property (IP), export controlled technology, and personally identifiable information (PII).

What's a Covered Transaction?

A proposed or pending transaction with any foreign person which could result in control of a U.S. business by a foreign person.

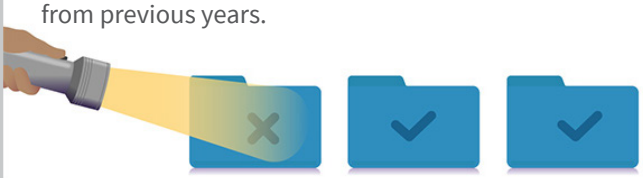
Source: CFIUS.

In 2019, CFIUS killed eight proposed deals, according to a report from Reuters. (A ninth deal was rejected personally by President Trump.) Throughout that year, the committee reviewed 231 transactions and performed in-depth investigations of 113 proposals.

Past deals are at risk, too. Since FIRRMA, CFIUS has transitioned from focusing primarily on reviewing notified transactions to aggressively researching and reviewing non-notified transactions from previous years. In some cases, the committee has launched formal government probes that have resulted in penalties and deal "unwinding."

Key Insight: Retroactive Review

CFIUS has transitioned from focusing primarily on reviewing notified transactions to aggressively researching and reviewing non-notified transactions from previous years.



That means that foreign-backed U.S. businesses with sensitive technologies or large amounts of PII (e.g., healthcare, aerospace and defense, financial services) could be on the receiving end of heightened government oversight and investigation. Foreign investors (e.g., private equity funds, sovereign wealth funds) may be forced to divest of certain investments. A chain reaction might ensue: Subsequent public media coverage of government investigations into certain funds or companies could inflict reputational damage and make it difficult for parties to close future deals.

Which brings us back to the precious commodity — data — and mitigating deal risk.

Understanding CFIUS' Cybersecurity Expectations

Every organization today is concerned about cyber attacks. Vulnerability is particularly acute since the pandemic accelerated remote working and increased the use of personal devices by employees. The explosive growth of cloud computing is also a factor. One estimate puts the average cost of a cyber breach in 2020 at $18.9 million per incident, up 5.3% over 2019.

Though many corporations recognize the need to tighten their cyber defenses, not all choose to act. They may be hampered by budgetary constraints, for one thing, or unaware of their specific cybersecurity gaps.

The way in which parties in a cross-border deal manage their cybersecurity is highly relevant to the scrutiny CFIUS can exercise under its extended authority.

Key Insight: Cybersecurity Stance

The way in which parties in a cross-border deal manage their cybersecurity is highly relevant to the scrutiny CFIUS can exercise under its extended authority.

For parties pursuing a deal, assessing cybersecurity posture is critical to meeting CFIUS' compliance expectations. That might seem straightforward, but it's easy to get caught in a web of potentially overlapping compliance and regulatory standards. Here are primary actions parties must consider:

- Conduct a regulatory gap assessment to identify necessary changes that need to be made to achieve compliance across export controls, data privacy, and cybersecurity obligations
- Assess the data environment, the control status of any sensitive technology, security infrastructure, and existing cybersecurity policies, procedure, and processes
- Design a control development and revision strategy that will recommend technology solutions, human resources protocol, and policy changes

Taking these actions can enhance an organization's compliance, data governance, and cybersecurity posture in general. They can further reduce corporate risk, cut storage costs, secure data, and improve the e-discovery process. However, parties pursuing an M&A should pay particularly close attention to these first moves, as cyber risk is often overlooked or given short shrift in the rush to close. Taking action early in the deal by proactively addressing vulnerable areas can not only put the deal on better footing should CFIUS come calling but can send a message of accountability to both the acquiring and target company.

For previously approved deals that have mitigation agreements in place, a thorough cybersecurity assessment will reveal where both parties stand with respect to CFIUS compliance and will reduce the risk of penalties and/or forced divestiture should they be investigated.

Protect Your Deal and Your Reputation

Beyond cybersecurity concerns, the importance of parties conducting due diligence in a cross-border deal extends to other issues that may be outside their control.

Key Insight: Ulterior Motives

Outside actors with their own motives are looking to take advantage of the newly aggressive CFIUS by seeking to influence its agenda. They can create legal, political and reputational risk for businesses and investors.

Within the regulatory environment, outside actors with their own motives are looking to take advantage of the newly aggressive CFIUS by seeking to influence its agenda. These actors may be business competitors, for instance, political stakeholders, or non-governmental organizations. Whatever their motivation, they seek to drive the narrative and can create more legal, political, and reputational risk for businesses and investors operating in critically sensitive sectors of the economy.

Foreign investors looking to buy or invest in U.S. assets must understand the political risks associated with the deal so they can manage and mitigate them.

For companies already in the throes of a CFIUS investigation, it's critical to have a sound communication, legal, and public affairs strategy in place to protect against reputational risks that can affect your freedom to invest — and to attract future investments.

Professional Assessment is Key

Performing due diligence across the entire CFIUS lifecycle can be a huge undertaking that includes improving cybersecurity, understanding political influence, assessing the export control status of your technology, preparing for and responding to an investigation, and bolstering compliance with mitigation agreements.

It's a complex landscape full of pitfalls that could trip up any investor or company. A professional assessment and strategy for managing the expectations and meeting CFIUS on its own turf is the way to get ahead of possible issues. It can also improve the odds that your deal will close — and stay closed.

Additional contributors to this article include: Johnny Xie, Eddie Lam, Beth Junell, Edward Bridges

AUTHORS

KYUNG KIM
Senior Managing Director

DAVID B. ROADY
Senior Managing Director

SALLY PENG
Managing Director

JOHN WHITCOMB
Managing Director