Overview
Institutions of Higher Education (IHEs) are increasingly finding themselves in the crosshairs of high-profile criminal enforcement efforts. Recent headlines have highlighted a number of investigations and prosecutions that have achieved literal celebrity status:

- The indictments and convictions of wealthy parents of college applicants in the Varsity Blues investigation, who are alleged to have paid bribes in order to gain their children's admission to prestigious colleges. (See, for example, our recent client alert on the latest Varsity Blues pleas.)
- The indictments and convictions of college coaches, sports agents, and sportswear company executives alleged to have paid bribes to students and their parents in exchange for commitments to play basketball at certain universities.
- The high-profile “Me Too” investigations into allegations by current and former students of sexual assault by college coaches and faculty members, including at Penn State, Michigan State, and other universities.

It may be that these investigations are aberrations, and that IHEs will ride gently into the sunset when these cases have reached their end. It is more likely, however, that with the media coverage of these investigations raising broader reputational concerns around IHEs, and prosecutors beginning to develop a deeper understanding of the way in which IHEs conduct their operations, these high-profile cases will instead usher in a new era of higher and broader law enforcement scrutiny against IHEs. The ever-increasing interactions and exchange of money between IHEs and the federal government and foreign government officials, together with their broadening involvement of IHEs in sensitive research and development efforts that affect both big business and national security, will only intensify that scrutiny.

As a consequence, university counsel must increasingly think less like education lawyers and more like a corporate compliance and investigative counsel. They understand the landscape of relevant criminal prohibitions across the institution’s operational areas and the attendant enforcement risks, tailor their compliance programs to address these risk areas, and be prepared to take appropriate investigative and, if necessary, remedial measures when concerns arise. In this alert, we highlight some of the primary areas of enforcement risk posed to IHEs.

Export Controls/Sanctions
Given the amount of research occurring at many IHEs and the international student body and faculty of such institutions, IHEs are increasingly subject to civil and criminal exposure under US export controls and sanctions law. US export controls compliance can be a difficult area for IHEs to navigate. The United States controls a variety of commodities, technology, and software, collectively known as “items,” for export, reexport, and transfer (in third countries). Dual-use items and certain less sensitive defense items are controlled by the US Department of Commerce, Bureau of Industry and Security (BIS) and are included on the Commerce Control List (CCL) as set forth in the Export Administration Regulations (EAR). More sensitive defense items are controlled by the US Department of State, Directorate of Defense Trade Controls, and are included on the US Munitions List (USML), which is part of the International Traffic in Arms Regulations (ITAR).
IHEs often encounter export control matters when dealing with “technology,” which is defined broadly under both the EAR and ITAR and may occur “in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection.”[1] The concept of an “export” is also broadly construed under both regimes and includes not only actual shipment or transmission of an item outside the United States, which may be applicable to universities with foreign-located satellite campuses, online learning that extends outside the United States, or working in partnership with other foreign institutions, but also the release or transfer of technology to a foreign person while within the United States. This latter concept is known as a “deemed export” and presents particular challenges for IHEs with international student bodies and faculties.

Of particular importance for IHEs, the EAR does not control “fundamental research,” which is defined to mean “research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.”[2] However, fundamental research does not extend to situations where “there are restrictions placed on the outcome of the research or restrictions on methods used during the research. Proprietary research, industrial development, design, production, and product utilization, the results of which are restricted and government funded research that specifically restricts the outcome for national security reasons are not considered fundamental research.”[3] Such scenarios might arise in the context of extra-curricular research projects or collaborations between universities and the private sector, among others. The EAR also excludes “printed books, pamphlets, and miscellaneous publications including bound newspapers and periodicals” and “information and software” that are “published,” which would generally cover information in textbooks and related materials.[4] The exact boundaries of this exemption and its limitations as applied in circumstances outside the classroom (such as sponsored internships, optional practical training, etc.), however, are not clear. Similarly, information and software “released by instruction in a catalog course or associated teaching laboratory of an academic institution” are not subject to the EAR.[5]

In addition to export controls, IHEs should also be aware of economic sanctions imposed by the US Department of the Treasury’s Office of Foreign Assets Control (OFAC). Such provisions prohibit or otherwise make sanctionable various activities with targeted persons, jurisdictions, and governments. Most US sanctions programs contain an exemption for the import and export of “information and informational materials” involving the sanctioned jurisdiction. However, this exemption does not apply in all circumstances, including with respect to certain items subject to US export controls. In addition, many US sanctions programs contain a general license permitting activities carried out in the United States “for which ... a visa has been granted by the US State Department or such nonimmigrant status or related benefit has been granted by the US Department of Homeland Security.”[6] This includes several types of visas commonly issued to students, including F (students) and J (exchange visitors) visas. There are nuances to how these visas operate as an OFAC authorization in certain programs where there may be carve outs or limitations, as well as in the current COVID-19 circumstances where visas may have been issued but actual travel to the United States for education is not possible.

BIS and DOJ have brought a number of related enforcement actions against universities and university professors in recent years. In 2015, the DOJ indicted the chair of Temple University’s physics department on four counts of wire fraud in an alleged scheme involving the exploitation of technology for the benefit of third parties in China.”[7] While the indictment did not allege specific violations of the EAR or ITAR, the wire fraud related to efforts by the professor to defraud a US company to obtain technology “so that he could provide it to entities in China and assist those entities in further exploitation and use of the technology.”[8] With respect to specific violations of the EAR, in 2013, BIS entered into a settlement agreement with the University of Massachusetts at Lowell to resolve two alleged violations of the EAR related to the export of atmospheric testing devices and related antennas and cables to a Pakistani entity on the BIS Entity List[9] without a required license. In 2008, a University of Tennessee professor was convicted of violating the US defense export control regime by, among the charges, transferring certain technology to non-US graduate students.

It is important for IHEs to carefully consider their activities that might implicate US export controls and sanctions and to implement appropriate policies and procedures to prevent violations. While criminal violations generally require intent or knowledge, civil violations of US export controls and sanctions can be enforced even if an actor is not aware their conduct may violate the law. Therefore, in addition to formulating policies and procedures, it is critical that such policies and procedures are implemented in practice and that relevant personnel receive appropriate training.

False Claims Act

As recipients of significant federal dollars, IHEs also must be mindful of their exposure to False Claims Act (FCA) liability. Although typically viewed as DOJ’s chief enforcement mechanism to combat health care and procurement fraud, DOJ has recently relied on the FCA to extract substantial settlements from IHEs and likely will continue to do so.
The FCPA is enforced criminally by DOJ and civilly against "issuers" by the US Securities and Exchange Commission. The FCPA prohibits bribery of foreign government officials and requires covered entities, including IHEs, to maintain complete and accurate books and records and adequate internal controls. IHEs, as recipients of billions of dollars in government funds through federal loan programs and grants, including research grants and federal Pell grants, are particularly susceptible to FCPA scrutiny. Recent FCPA settlements and case law signal to recipients of federal monies, including IHEs, that DOJ can and will pursue FCPA actions associated with the submission of claims made in connection with the receipt of federal funds that fail to disclose violations of statutory, regulatory, or contractual conditions of program eligibility or payment.

In recent years, FCPA actions against IHEs have focused on "abusive" student recruiting practices, zeroing in on for-profit institutions that fraudulently certify compliance with the Higher Education Act of 1965 (HEA), which aims to eliminate the practice of recruiting students regardless of their qualifications to secure student-aid funds from the federal and state governments by prohibiting IHEs from using incentive-based systems to pay admissions personnel. In 2015, for example, Education Management Corp. agreed to a $95.5 million settlement to resolve allegations that it falsely certified compliance with the HEA.

The Foreign Corrupt Practices Act (FCPA), which prohibits bribery of foreign government officials and requires covered persons to maintain complete and accurate books and records and adequate internal controls, is another US federal statute that can present risks for IHEs. IHEs need to compete for grants from sources associated with foreign governments, and, per-violation penalties, ranging from $11,665 to $23,331. In addition to these stiff financial consequences, FCA violators can also suffer substantial reputational harm.

While many FCA actions are initiated by DOJ, the FCA is a somewhat unique enforcement statute in that it permits whistleblowers (typically individuals within an organization) to report wrongdoing they believe they have witnessed through the filing of qui tam suits. As a mechanism to encourage these suits, whistleblowers (referred to as relators) in successful FCA suits can be awarded anywhere from 10% to 30% of the final recovery, plus attorneys' fees.

There has also been aggressive FCA enforcement in the area of federal research grants. Notably, the $3 billion recovered by DOJ under the FCA in 2019 included a hefty $112.5 million settlement with Duke University to resolve allegations that the university knowingly submitted to the National Institutes of Health and the Environmental Protection Agency, applications and progress reports under 30 federal research grants that included falsified research and data.

On the most immediate horizon lies potential DOJ enforcement efforts against IHEs related to the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which provides $14 billion for post-secondary institutions through the Higher Education Relief Fund. Section 18004 of the CARES Act requires that IHEs use no less than 50% of funds received "to provide emergency financial aid grants to students for expenses related to the disruption of campus operations due to coronavirus (including eligible expenses under a student's cost of attendance, such as food, housing, course materials, technology, health care, and child care)," and obligates IHEs to submit reports to the Secretary of Education describing the institution’s use of funds.

The infusion of CARES Act funding in addition to the billions of federal dollars already received by IHEs provides another reason for these institutions to carefully review their compliance procedures to ensure that representations made to the federal government in connection with the receipt and use of funds are accurate and reflect compliance with obligations associated with that funding.

**FCPA**

The FCPA is enforced criminally by DOJ and civilly against "issuers" by the US Securities and Exchange Commission (SEC). It comprises two sets of provisions:

1. Anti-bribery provisions, which apply to (a) "domestic concerns," namely US citizens, nationals, or residents and entities organized or headquartered within the United States, as well as officers, directors, employees, agents, or stockholders acting on behalf of such entities, using interstate commerce; (b) US nationals and entities organized within the United States, even if no interstate commerce is used; (c) "issuers" of securities traded on a US stock exchange, as well as any officer, director, employee, or agent of an issuer, or a stockholder acting on the issuer's behalf, using interstate commerce; (d) any other person (including non-US persons and entities) engaged in acts to further corrupt schemes while in US territory; and;

2. Accounting provisions, including record-keeping and internal control requirements, which apply only to "issuers."
Although most traditional US IHEs (in contrast with certain publicly traded, for-profit IHEs) are not "issuers," they—along with their administrators, professors, and staff—are domestic concerns and therefore subject to the FCPA's anti-bribery provisions. In addition, while non-issuer IHEs are not subject directly to the FCPA’s accounting provisions, compliance with such provisions is nonetheless a best practice and may help prevent violations of the FCPA’s anti-bribery provisions, other criminal laws, and various contractual requirements.

The FCPA’s anti-bribery provisions prohibit corruptly offering, promising, or providing "anything of value," directly or indirectly, to a "foreign official" to secure official action, inaction, or influence to assist "in obtaining or retaining business for or with, or directing business to, any person ...." Under the FCPA, "anything of value" is interpreted broadly and, with respect to IHEs, might include favorable treatment for officials and their relatives with respect to admissions; grants and scholarships; financial assistance; charitable and political contributions; travel and hospitality; and hiring and internships, among other items of value.

"Foreign official" includes not just elected or appointed officials and their staffs (from any branch and level of government) but also employees of instrumentalities, officials of public international organizations, and individuals acting in an official capacity on behalf of a government, instrumentality, or public international organization. Notably, for IHEs, this includes officials and employees of public universities, hospitals, and research institutes, in addition to foreign officials from education ministries and other governmental bodies with whom universities and colleges might interact.

The phrase "obtaining or retaining business" also is interpreted broadly to include winning new or additional business and receiving a broad range of other business benefits or advantages. In the context of higher education, this might include seeking accreditation for foreign campuses and joint degree programs; seeking other licenses, research permits, visas, and regulatory approvals; seeking favorable inspection results from health/safety, labor, or other authorities; seeking donations and grants from foreign governments; entering research collaborations and licensing arrangements with foreign universities, hospitals, and research institutes; lobbying for advantageous laws or regulations; and resolving litigation, disputes, and assessments; among other business benefits.

Apart from being responsible for bribery by an IHE's own personnel, an IHE also can be vicariously liable for third-party conduct when the IHE disregards red flags signaling a high likelihood the third party will pay bribes on its behalf. Historically, third-party conduct has given rise to the majority of FCPA enforcement actions. Third parties may include, for example, an IHE's recruiting and other agents, consultants, contractors, service providers, and other business partners, with heightened risk surrounding any third party that will interact with the government on the IHE's behalf or that is owned or otherwise affiliated with a government official in a position to confer benefits on the IHE.

Recent enforcement actions involving the offer or provision of employment, internships, or scholarships to family members of government officials, charitable contributions, and leisure trips and hospitality allegedly to obtain a variety of business benefits from foreign governments, offers a strong indication as to how DOJ would view an IHE's offer of similar items of value to government officials or their relatives when the officials are in a position to confer benefits to the IHE in return. While there has not yet been a published FCPA enforcement action involving IHEs, they have been subject to FCPA investigations. For example, in December of 2016, Laureate Education Inc. (Laureate), the largest operator of for-profit higher education schools, disclosed it was investigating an $18 million charitable donation in Turkey, including whether any of the money was diverted to government officials or such officials' encouragement in order to enhance the position of the company within Turkey. Laureate disclosed the matter to the DOJ and SEC, which later concluded investigations into the matter without further action.

IHEs' implementation of a robust anti-corruption compliance program—including appropriate, risk-based policies and procedures; training; compliance structures; third-party due diligence, contractual protections, and monitoring; and mechanisms for seeking guidance and for reporting and investigating concerns—is important for IHEs to mitigate risk under the FCPA and other anti-corruption laws. Such a program can help prevent potential violations from occurring. And, if a violation does occur, implementation of an effective compliance program will be considered by the DOJ when determining whether to bring an enforcement action and mitigates otherwise applicable penalties under the US Sentencing Guidelines.

**Trade Secret Theft & Foreign Influence**

Over the last few years, DOJ has also stepped up investigations and enforcement related to alleged thefts of trade secrets and false statements regarding foreign funding. Many of its cases have focused on researchers working at IHEs.

**Trade Secret Theft**

A trade secret is confidential business information with actual or potential economic value—i.e., information that can provide a competitive advantage. Prototypical examples include the formula for Coca-Cola and advanced technology like self-driving car plans. Certain information commonly found at universities, including information arising out of university-sponsored scientific research, as well as information proprietary to the university, such as admissions data and potentially even athletic scouting reports, may also qualify as trade secrets.
Theft of trade secrets can be prosecuted at the federal and state level, and both federal and state prosecutors have numerous tools at their disposal to enforce criminal trade secret theft. The Economic Espionage Act, which applies to trade secret theft to benefit a foreign government or affiliated entity, has recently become a popular tool for federal prosecutors.

Under the Trump administration, the DOJ has been particularly focused on trade secret theft involving Chinese nationals. On November 1, 2018, DOJ announced its "China Initiative," which focuses on preventing and prosecuting thefts of American technology and intellectual property for the benefit of China from "non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to US interests." As part of this initiative, DOJ has turned its attention to prosecuting trade secret theft at universities. For example, DOJ recently charged a Chinese visiting professor at the University of Texas, Arlington for allegedly stealing US technology to benefit a Chinese technology company.

Despite DOJ’s focus, prosecutors do not always understand the underlying technology, which has resulted in high-profile blunders. For example, in May 2015, FBI agents arrested the interim chair of Temple University’s physics department for sharing sensitive information about a superconductor device with Chinese scientists. DOJ dropped the charges only months later, acknowledging that the blueprints he shared with Chinese researchers were for a completely different device and were already public.

Foreign Influence

DOJ has also used federal reporting requirements applicable to IHEs and researchers and general criminal statutes to address concerns about economic espionage and foreign influence at IHEs. It has charged academics with wire fraud, false statements, and federal programs fraud for conduct involving funding from China or undisclosed conflicts of interest. IHEs and researchers are required to report certain foreign ties. For example, Section 117 of the Higher Education Act requires IHEs that receive federal funding to report gifts from or contracts with a "foreign source" totaling more than $250,000 in a year. Although this provision was enacted more than 20 years ago, the Department of Education has only recently started to enforce the provision aggressively. Other agencies, such as the National Institutes of Health (NIH) have issued similar regulations requiring researchers who receive federal funds to report information relevant to financial conflicts of interest, including funding received from foreign sources. Although these reporting obligations do not create independent criminal exposure, false statements provided to the federal government in required disclosures or in the course of subsequent investigations could result in federal charges. Depending on the underlying conduct, parallel criminal investigations could also result in fraud or other charges.

DOJ has focused in particular on the Thousand Talents Program, a Chinese government program with the goal of improving China’s access to talent, research, and technology. In one high-profile case, DOJ charged the chair of Harvard’s chemistry department with making false statements to Defense Department investigators when he denied being asked to participate in the Thousand Talents Plan. The government alleged that the nanotechnology expert had, in fact, signed a contract to work for a Chinese university in exchange for as much as $50,000 a month in addition to living expenses and grant money. In other cases, the government has charged individuals associated with institutions such as Emory University, Virginia Tech, the University of Kansas, and West Virginia University with wire fraud, federal programs fraud, tax fraud (for failing to report foreign income), and making false or misleading statements to federal agencies regarding funding from China or conflicts of interest.

Although most enforcement actions have focused on individuals in cases where IHEs were (at least arguably) victims, a recent case suggests an expectation that IHEs bear some responsibility for taking steps to prevent their employees from violating these statutes. In December 2019, DOJ announced that it had reached a civil settlement with the Van Andel Research Institute (VARI) to resolve allegations that the biomedical research institute had violated the FCA by submitting grant applications and other documents to NIH that failed to disclose Chinese governmental grants provided to two VARI researchers, including through the Thousand Talents Program.

Similar prosecutions can be expensive for universities, which may be required to produce documents in response to a grand jury subpoena and have employees sit for interviews with the DOJ. These cases underline the need for IHEs to take the following steps to protect their intellectual property and ongoing research projects, their reputations, and their limited resources:
• Perform robust vetting of new hires that will have access to sensitive information or research, for possible ties to foreign
governments.
• Identify existing and planned foreign funding sources to determine whether they are permissible and consistent with the
terms in any grants received from the US government.
• Educate faculty and students about the laws surrounding trade secret theft and foreign funding.
• Ensure adequate measures are in place to protect sensitive data, including passwords, encryption, and firewalls.
• Consider forming committees to review sensitive research projects that present elevated compliance risks.[41]
• If a possible trade secret theft or other misconduct is suspected, promptly have counsel conduct an internal
investigation to assess the scope and mitigate the risk to the institution.[42]

With IHEs’ continued expansion their international footprints and their receipt of millions of dollars in grants and loans from
both the federal government and international sources, they are operating more like global businesses now more than
ever before. As such, they must approach law enforcement risk management accordingly. It is more important now than
ever that in-house counsel and compliance managers have at their disposal not only the subject-matter expertise in the
areas discussed herein, but also the ability to craft and maintain robust compliance programs in these areas, to conduct
thorough (but cost-efficient) investigations in to allegations of potential criminal misconduct, and to navigate the complex
issues of disclosure and cooperation with DOJ[43] and other relevant agencies (such as the Department of Education)
when it has concluded upon investigation that criminal misconduct is likely to have occurred.

[7] US Dep’t of Justice, Press Release, University Professor Charged In Wire Fraud Scheme (May 21, 2015), available at:
[8] Id.
[9] Export, reexports, and transfers (in-country) to persons on the Entity List, contained in Supplement No. 4 to Part 744 of
the EAR, are subject to enhanced licensing requirements and generally may not utilize license exceptions contained in
the EAR. There are a number of universities located in China and elsewhere that are on the Entity List.
[12] Parties, however, are free to and often do negotiate lower damages as part of settlement agreements.
[16] See United States v. Esquenazi, 752 F.3d 912, 925 (11th Cir. 2014), cert denied 135 S. Ct. 293 (2014) (adopting a
two-prong test to determine whether an entity or operation was an “instrumentality” based upon (1) whether the
government in question controls the state-owned entity (SOE) in question, and (2) whether the functions that the SOE
performs are ones that the foreign government “treats as its own”).


[24] For example, in July 2002, Yale University discovered that a Princeton admissions staffer was using Princeton applicants’ social security numbers to check a Yale website that notified students whether they had been admitted. Yale quickly involved the FBI, which led Princeton to temporarily suspend the staffer involved. See Arielle Levin Becker & Elise JordanFBI to investigate Princeton admissions hacking incident, Yale Daily News (July 26, 2002), available at: https://bit.ly/2zHv7MH; Pallavi Mathur, Claiming Admissions Data Trade Secrets


"False statements" refers to 18 U.S.C. § 1001, which criminalizes false statements to the US Government. This statute is distinct from the False Claims Act theories discussed above.


Press Release, US Dep't of Justice, Department Of Justice Reaches $5.5 Million Settlement With Van Andel Research Institute To Resolve Allegations Of Undisclosed Chinese Grants To Two Researchers (Dec. 19, 2020) https://www.justice.gov/usao-wdmi/pr/2019_1219_VARI. The government alleged that VARI made certain representations with deliberate ignorance or reckless disregard for the truth regarding that funding from China. (See infra for further discussion regarding the False Claims Act).


Some individual defendants have tried to force their employers to pay their fines. The defendant in the dispute between Google and Uber, for example, has tried to make Uber responsible for the $179 million award against him. See Timothy B. Lee, Uber accuses Levandowski of fraud, refuses to pay $179M Google judgment, Ars Technica (April 20, 2020), available at: https://arstechnica.com/cars/2020/04/uber-accuses-levandowski-of-fraud-refuses-to-pay-179m-google-judgment/. In other cases, employment contracts may require indemnification or the advancement of legal fees.

For discussion of DOJ's formally issued guidance on the benefits of voluntary disclosure and cooperation, see our prior client alerts.

Practices
Independent & Internal Investigations

White-Collar Defense

© 2020 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.