Corporate Crime, Internal Investigations and the Duty to Report

Matthew Krueger
United States Attorney, E.D. Wisconsin

Tom Kister
Legal Director, Johnson Controls Federal Systems, Inc.

Stacy Gerber Ward
von Briesen & Roper, s.c.

Wisconsin Ethics Rules

- Rule 1.2(d) **Scope of Representation**

  A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

Wisconsin Ethics Rules

- Rule 1.13(b) **Organization as Client**
  - If a lawyer for an organization knows that **an officer, employee or other person associated with the organization** is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law which reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer **shall proceed as is reasonably necessary** in the best interest of the organization.
  - Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances, to the highest authority that can act in behalf of the organization as determined by applicable law.

Wisconsin Ethics Rules

- ABA Formal Opinion 491 (4/29/20)
  - Obligations to Avoid Counseling or Assisting in a Crime or Fraud
  - Rule 1.2(d) states that a lawyer **shall not assist** in criminal or fraudulent conduct
  - Standard includes “actual knowledge”
  - Knowledge also includes when the “facts before the lawyer indicate a **high probability**” that the client seeks to use the lawyer’s service for a prohibited activity
  - Duty to consult with client on the limitations on the lawyer’s conduct

DOJ and Corporate Enforcement

- DOJ Key Enforcement Areas
  - False Claims Act
  - Foreign Corrupt Practices Act
  - Health Care Fraud
  - Market Integrity (Securities and Accounting Fraud)
- DOJ Policy on Cooperation and Compliance Programs
- DOJ Policy on Avoiding Duplicate Criminal/Civil Recoveries
- DOJ Assistance for Corporations

FBI/DOJ Intellectual Property Initiative

- The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is between $225-$600B.
- The Chinese government is the world's principal infringer of intellectual property, and it uses its laws and regulations to put foreign companies at a disadvantage and its own companies at an advantage.
- U.S. business interactions with foreign counterparts should be based on the principles of reciprocity, should be grounded in the rule of law, and should seek to uphold our market-based economy and its innovative ecosystem.
- The Chinese government, however, does not play by the same rules.

FBI/DOJ Initiative

- Made in China 2025 Plan
- To support its military and commercial research, development, and acquisition, the Chinese government leverages:
  - Foreign investments,
  - Commercial joint ventures,
  - Business relationships originating from academic exchanges, and
  - State-sponsored industrial and technical espionage.

2019 National Defense Authorization Act

- In §889 of this Act, Congress and the President determined that certain telecommunications and video surveillance equipment made in China poses a national security risk.
- Part A was effective on August 13, 2019 and prohibited contractors from **supplying** these banned products and services for U.S. Government end users.
- Part B was effective on August 13, 2020 and generally prohibited U.S. Government contractors from **using** banned products and services in their own operations.
- Affected companies include: Huawei, ZTE, Hytera, Hikvision, Dahua, Hisilicon, and their subsidiaries.

Insider Threats

Insider Threat Risks

Your company is vulnerable to damage from an insider—an employee who has legitimate or illegitimate access to company information and provides that information to a foreign adversary. Insider threats could begin as early as the job application phase, where applicants might be directed by foreign governments to seek employment with access to U.S. trade secrets or proprietary information.

Some of these behaviors might indicate an employee potentially poses an insider threat risk to your company:

- Displays suitability issues, such as alcohol abuse or illegal drug use
- Insists on working in private
- Volunteers to help on classified or sensitive work
- Expresses an interest in covert activity
- Has unexplained or prolonged absences
- Is disgruntled to the point of wanting to retaliate against the company
- Rummages through others' offices or desks
- Misuses computer or information systems
- Unnecessarily photocopies sensitive material
- Attempts a computer network intrusion
- Has criminal contacts or associates
- Employs elicitation techniques
- Displays unexplained affluence
- Fails to report overseas travel, if required
- Works unusual hours
- Takes classified or sensitive material home
- Conceals foreign contacts
- Lacks concern for or violates security protocols
- Attempts to gain access without a need to know
- Shows unusual interest in information outside the scope of his or her job

U.S. v. Sinovel Wind Group (W.D. Wis.)

- AMSC had offices in Wisconsin; made electrical components for power wind turbines
- Sinovel was a Chinese corporation that made wind turbines and was AMSC's biggest customer
- Sinovel intentionally recruited an AMSC engineer to steal trade secrets for Sinovel
- After Sinovel obtained the technology, it no longer needed AMSC and broke off the business relationship. AMSC's business suffered, with 600 employees being laid off

U.S. v. Sinovel Wind Group (W.D. Wis.)

- AMSC worked with the FBI and DOJ in the investigation. DOJ protected AMSC by using a protective order that limited any trade secrets from being disclosed in discovery.
- Jan. 2018, Sinovel became the first Chinese corporation convicted in a U.S. court for trade secret violations.
- July 2018 sentencing resulted in the max. statutory fine ($1.5M) and restitution of $57.5M, which has been paid.

The Role of Corporate Compliance

- Traditionally understood to act as a watchdog for organization's internal compliance with laws, regulations, and ethics policies.
- But also may surface concerns about internal or external threats to an organization (overlap with risk management).
- Mature compliance programs can see over the horizon and raise issues that can give a company a competitive advantage over its competition.
- Many corporate compliance officers are lawyers and subject to state ethics rules for not facilitating crime or fraud and protecting the organization from illegal activities of officers/directors.

Elements of an Effective Compliance Program

- Clearly written codes, policies, and procedures
- Tone at the top (and the middle)
- Access to senior company executives
- Real non-retaliation
- Multiple (and well publicized) reporting avenues
- Continuous examination and improvements
- Multimodal training modules
- Consistent enforcement

Know your Customers, Your Vendors, and Your Targets

- Customers
  - Are the who they present themselves as?
  - What are their operations and what are they asking of you?
- Vendors
  - Identify your high risk vendors – those who act on your behalf or as your agents.
  - International concerns under Foreign Corrupt Practices Act and other similar statutes of other countries
- Targets (M&A)
  - Don’t buy your way into a compliance investigation – do your diligence on who you are targeting for acquisition or merger

Internal Investigations

- Obligation to protect the organization per Rule 1.13(b)
  - Lawyer **shall proceed as is reasonably necessary** in the best interest of the organization
- Principals of internal investigations
  - Consider attorney-client privilege
  - Tailored but thorough
  - Identify possible wrong-doers in the organization
- To Report or Not to Report. . .