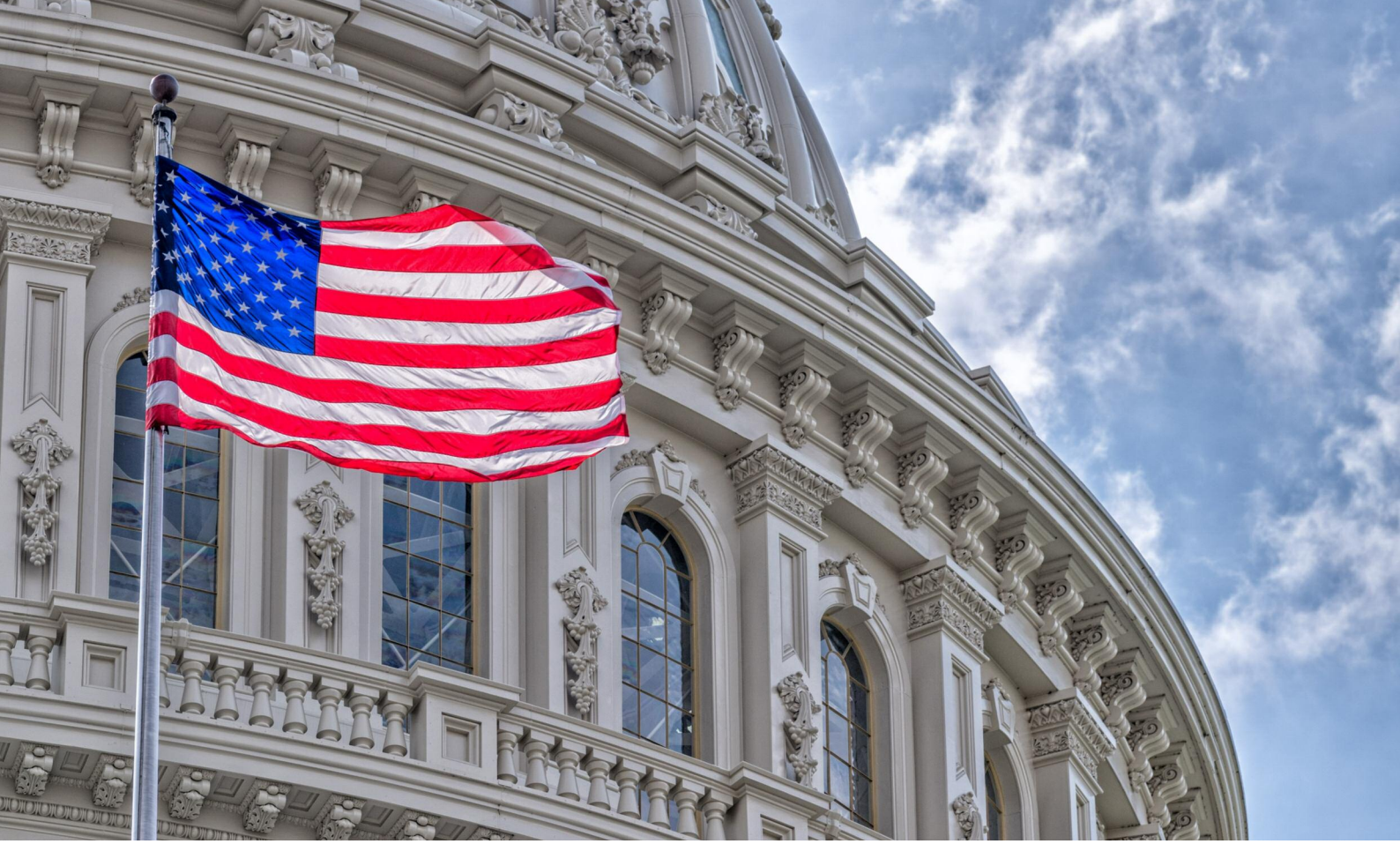
MANAGING INVESTIGATIONS

Best practice in Government and Internal Investigations

A WORLDECR GLOBAL GUIDE

reprinted with permission
WWW.WORLDECR.COM



USA

by Dj Wolff and Derek Hahn, Crowell & Moring

www.crowell.com

INTRODUCTION

With an expansive legal framework, aggressive regulatory authorities, and severe potential penalties, US international trade laws continue to be some of the most complex and consequential in the world. The rise in inter-agency and international coordination continues to exacerbate this complexity, amplified by the exponential growth of relevant data sources and volumes, and the difficulty of accessing them – both technically and legally. Year after year, US regulators announce record-setting enforcement actions against both companies and individuals. And US regulators are increasingly touting the benefits of voluntary self-disclosures, forcing companies to grapple with this vexing decision with a growing regularity when conducting internal investigations.

In short, the difficulty of successfully conducting US international trade law investigations has never been greater, and the financial – and reputational – stakes have never been higher. This chapter is

intended to provide a practical overview of this enforcement landscape, and the key investigatory issues faced by those hoping to successfully navigate it.

THE AGENCIES AND COMPETENT AUTHORITIES

What agency or agencies may be involved in an investigation for sanctions, export control, anti-corruption or AML violation?

In the United States, a wide array of enforcement agencies are responsible for administering sanctions, export control, anti-corruption, and AML laws. The primary enforcement authorities for key federal statutes in each area are described below. This is an area in which US state-level authorities, from the individual state criminal prosecutors (e.g., the Manhattan District Attorney's office) to state-level civil regulators (e.g., the New York Department of Financial Services ('DFS')) can also play a role, pursuing both independent and coordinated enforcement actions with their federal colleagues. Because of the number of permutations that arise across 50 states, this chapter focuses primarily on US federal regulators, except where noted.

Sanctions

The Department of Treasury's Office of Financial Assets Control ('OFAC') is the primary US civil regulator for sanctions enforcement. A limited set of sanctions are overseen by the US Department of State.

The National Security Division of the Department of Justice ('DOJ') is responsible for prosecuting criminal violations of the primary US export control and sanctions statutes: including, but not limited to, the Arms Export Control Act ('AECA'),[1] the Export Control Reform Act ('ECRA'),[2] the International Emergency Economic Powers Act ('IEEPA'),[3] and the Trading With the Enemy Act ('TWEA').[4] DOJ regularly works with its US Attorneys' Offices and the Federal Bureau of Investigation ('FBI'), among other agencies, to conduct investigations.

David (Dj) Wolff is a Partner within Crowell & Moring's International Trade Group and a director with C&M International, the firm's trade policy affiliate

Derek Hahn is a partner in the firm's White Collar & Regulatory Enforcement Group and a member of the firm's Investigation Practice.

www.crowell.com

Export control
The US export control regime is primarily overseen by two regulators: the US Department of State's Directorate of Defense Trade Controls ('DDTC'), which oversees the International Traffic in Arms Regulations ('ITAR'), and the US Department of Commerce's Bureau of Industry and Security ('BIS'), which oversees the Export Administration Regulations ('EAR'). Criminal prosecutions are overseen by DOJ as discussed above.

Anti-corruption
The Foreign Corrupt Practices Act ('FCPA')[5] is the primary US statute used to regulate corruption in international trade with a US jurisdictional nexus. DOJ and the US Securities and Exchange Commission ('SEC') are jointly responsible for enforcing the FCPA.

International corrupt conduct can give rise to enforcement actions by other US enforcement authorities as well. For example, on 6 March 2019, the Commodity Futures Trading Commission ('CFTC') Division of Enforcement announced its intention to prosecute violations of the Commodity Exchange Act carried out through foreign corrupt practices.[6] The CFTC resolved its first enforcement action involving foreign corruption in December 2020 against Vitol, Inc., with DOJ resolving a parallel criminal action the same day.[7]

AML
The primary US money laundering statute is the Bank Secrecy Act ('BSA'),[8] which is overseen by the US Department of the Treasury's Financial Crimes Enforcement Network ('FinCEN'). Criminal violations of the BSA are pursued by DOJ's Money Laundering and Asset Recovery Section ('MLARS').

What are the investigatory powers afforded to those agencies?

US authorities have varying investigatory powers, typically including the power to compel the production of both documents and testimony. Some agencies, such as the DOJ, may engage in more aggressive investigatory measures – including wiretaps and search warrants – upon demonstrating sufficient cause to a judicial authority.

THE INVESTIGATION: KEY QUESTIONS AND ACTIONS

What are the respective responsibilities of external counsel, consultants and in-house compliance/legal officers?

It is common in the United States for attorneys to direct investigations to maximise application of the attorney-client privilege and attorney work product doctrine. These privileges can be used to protect sensitive internal investigation materials from compelled disclosure.

Outside counsel, when involved, generally take the lead on most investigative activities to leverage the benefits of their expertise and support application of the attorney-client privilege. They are also the primary, and often exclusive, point of contact for investigating government agencies.

Various types of third-party consultants are used in US investigations. For example:

- E-discovery firms forensically collect and host data for review by the investigation team.
- Forensic accountants and other subject matter experts analyse and interpret specific types of data, review policies and procedures to identify and design related remedial measures and compliance programmes, and assist with other complex investigative activities.
- Due diligence companies perform background research on corporations or individuals implicated in the investigation.

In-house counsel and compliance officers typically work closely with outside counsel throughout the investigation, such as by:

- Assisting with the identification and collection of documents and information;
- Identifying relevant personnel and potentially participating in interviews;
- Providing input on the investigation scope, supporting activities, and results;
- Developing and implementing remedial actions;
- Helping coordinate updates to the company's external auditors, interactions with third-party business partners, or disclosures to lenders or public markets; and
- Strategising about the approach to the relevant government authorities, including voluntary or mandatory disclosures, and proposed resolutions.

In international investigations, local counsel in the relevant jurisdictions may be retained to advise on local laws, including those related to local export control, sanctions, and AML requirements, data privacy, and employment and/or labour issues.

At what point is it advisable to appoint outside counsel in the conduct of an investigation?

Whether an investigation warrants the retention of outside counsel is case-specific and depends on factors such as:

- The significance of the potential civil, criminal, and collateral exposure;
- The complexity of the factual and legal issues;
- The experience, expertise, and bandwidth of the company's in-house legal and compliance resources;
- Whether the company's in-house resources are implicated in the investigation;
- The likelihood that disclosures or other interactions with government regulators will be required; and
- The likelihood of a government investigation or related enforcement action.

Given the fast-changing and complex interplay of US regulations in this area as well as the substantial financial and reputational risks of violations (discussed below), outside counsel with subject matter

expertise in the regulations are often called upon more routinely by clients for even seemingly straightforward reviews than they may be in other regulatory areas.

Where an investigation warrants the retention of outside counsel, it is best to do so at the outset. This enables outside counsel to assist with the critical decisions that arise in the beginning of an investigation, some of which may be difficult to adjust down the road – including preservation of applicable privileges, avoiding unnecessary admissions, and seizing opportunities to make timely disclosures.

ADMINISTRATIVE AND PROCEDURAL REQUIREMENTS AND BEST PRACTICE

What records is it advisable or mandatory to keep that may be useful or essential in the event of an investigation?

Several of the international trade laws in the US have specific requirements to maintain records. They include:

Sanctions
OFAC requires parties to keep 'a full and accurate record' of every transaction engaged in subject to its authority for a five-year period from the date of the transaction.[9] Records related to blocked property must be kept for five years after the date on which the property is unblocked, often resulting in a total retention period substantially in excess of five years.[10]

Export controls
In contrast to OFAC's generally worded requirement, BIS delineates a series of documents that parties are specifically required to retain, including, *inter alia*: (1) licences, licence applications, and all supporting documents; (2) electronic export information ('EEI') on the Automated Export System ('AES'); (3) bills of lading; (4) all documents submitted as part of the export clearance process; (5) underlying contractual documents; and (6) specific records required by certain export provisions or licence exceptions (e.g., end-use certificates).[11] BIS also requires records to be kept for five years from the export or any known re-export or transshipment of the item.[12]

> **'OFAC requires parties to keep 'a full and accurate record' of every transaction engaged in subject to its authority for a five-year period from the date of the transaction.**

Anti-corruption
Companies subject to the FCPA's accounting provisions are required to make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect their transactions and dispositions of assets.[13] In addition, DOJ's FCPA Corporate Enforcement Policy makes clear that it expects companies to appropriately retain business records, including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms.

AML
FinCEN similarly maintains a detailed list of records that financial institutions must retain, including, with respect to each financial flow, *inter alia*: (1) the name and address of the transmitter; (2) the amount and date of the order; (3) any payment instructions received; (4) the identity of the recipient and its financial institution; and (5) other specific information received as part of the transmission.[14] FinCEN maintains more detailed record-keeping requirements for certain types of transactions as well as for certain types of financial institutions, but in all cases requires records be retained for five years.[15]

In addition, the following types of records are often helpful to assist with an investigation or in the negotiation of a resolution:

- **Policies and procedures** – e.g., compliance policies, delegation of authority matrices, transaction approval procedures, documentation of the purpose and scope of the evolution of those policies and procedures, evidence of tone from the top and middle in support of the policies, related risk assessments, and associated training records;
- **Transactional documentation** – e.g., contracts and related evidence of performance and market value of compensation, purchase orders / invoices, approval documentation, accounting data, and related entries in databases, ERP systems, etc.;
- **Vendor onboarding files** – e.g., credit checks, screening results, third-party due diligence reports, business references, questionnaires and follow-up inquiries, certifications, and documentation of termination or rejection of vendors with unresolved flags or adverse investigation findings etc.; and
- **Investigation, audit, and remediation records** – e.g., documentation of the results of investigations, audits, and related remedial measures, e.g., employee discipline, changes in policies or procedures, etc.

In addition, at the outset of an investigation, all relevant records should be preserved using techniques such as the issuance of hold orders, back-end electronic holds, and source-specific collections.

Is it mandatory to allocate legal responsibility for the company's actions to a named officer?

It depends on the subject matter area as to whether it is a legal requirement, or simply a recommendation. For example, the strictest requirement is within the AML regime, where FinCEN requires as part of a regulated entity's AML programme the 'designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance.'[16] DDTC maintains a slightly less affirmative requirement, instead requiring only that each registered company identify an 'Empowered Official' with

authority to sign licence applications or requests for approval on behalf of the applicant.[17] There is no legal requirement under OFAC, BIS, or the FCPA to allocate legal responsibility to a named officer. However, they often strongly encourage the identification of a specific officer. For example, in guidance, OFAC has identified the appointment of a 'dedicated OFAC sanctions compliance officer' as an element in an effective sanctions compliance programme.[18]

In addition, the United States Sentencing Guidelines also consider, in some scenarios, whether the individual or individuals with operational responsibility for the compliance and ethics programme have direct reporting obligations to the governing authority or an appropriate subgroup, such as the audit committee of the board of directors.[19]

Is the possession of an internal compliance programme ('ICP') regarded as potential mitigation in the event of a finding of violation?

Yes. US enforcement authorities uniformly regard an effective ICP as an important mitigating factor in corporate resolutions. Even companies which did not have an effective ICP at the time of the offence can often receive credit for improving an existing programme, or implementing one for the first time.

For example, when determining whether to charge a corporation or otherwise negotiate a criminal resolution, DOJ will consider 'the adequacy of and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision.'[20]

Other US authorities have adopted similar positions in the civil context. The SEC recognises efforts at 'self-policing prior to the discovery of the misconduct, including establishing effective compliance procedures' as well as 'remediation, including . . . modifying and improving internal controls and procedures to prevent recurrence of the misconduct [.]'[21] And BIS's Office of Export Enforcement ('OEE') will take account of the nature and adequacy of a company's BIS compliance programme at the time of a violation, and the company's remedial response – including 'whether it adopted new and more effective internal controls and procedures to prevent the occurrence of similar apparent violations.'[22]

OFAC's Enforcement Guidelines similarly recognise the 'existence, nature and adequacy of a [regulated] person's risk-based OFAC compliance program' as a key determinant in assessing whether and how to pursue an enforcement response.[23]

"Voluntary self-disclosureshave long been seen as a mitigating factor in US investigations, and are expressly recognised as such under the US Sentencing Guidelines.

What is best practice/regulatory obligation regarding voluntary disclosure in the US? Is it regarded as a mitigation if a company makes a voluntary disclosure?

Setting aside mandatory reporting obligations that are not tied to identified violations (e.g., reporting of rejected or blocked transactions to OFAC[24] or financial institutions' suspicious activity reporting to FinCEN[25]) as well as general mandatory reporting obligations that are not tied specifically to this subject area (e.g., government contracts-related mandatory disclosures),[26] there is only one circumstance in which disclosures of a known violation are mandatory under US export control, sanctions, and AML requirements. Specifically, any person who knows or has reason to know of a sale, export, or transfer of articles, services, or data subject to the USML to an arms-embargoed country (known colloquially as '126.1 Countries' for the provision in the regulations that identifies them) is required to immediately inform DDTC.[27]

However, in each of these regulatory areas, US agencies allow for and strongly encourage voluntary self-disclosures ('VSDs'). VSDs have long been seen as a mitigating factor in US investigations, and are expressly recognised as such under the US Sentencing Guidelines.[28] In recent years, US regulators expanded efforts to promote VSDs by publishing guidance outlining the requirements to obtain credit for such disclosures and the benefits to be gained. For example:

- DOJ adopted a FCPA Corporate Enforcement Policy that governs VSDs of FCPA violations, and that serves as non-binding guidance in other criminal matters. The CFTC similarly issued an advisory on self-reporting and cooperation for Commodity Exchange Act ('CEA') violations involving foreign corrupt practices.
- DOJ's National Security Division issued an Export Control and Sanctions Enforcement Policy for Business Organisations that encourages VSDs of wilful violations of the primary export control and sanctions regimes.
- The civil regulators maintain similar provisions encouraging VSDs. OFAC, for example, grants an automatic 50% deduction from any civil penalty disclosed through a VSD.[29] The SEC,[30] BIS,[31] DDTC,[32] and FinCEN[33] all similarly encourage VSDs.

In general, voluntary disclosures must satisfy three criteria to receive credit:

- The disclosure must be *voluntary*, meaning it occurs prior to the imminent threat of the violation otherwise coming to the government's attention (e.g., a disclosure may not be considered voluntary if a whistleblower is threatening to tell the authorities about the violation at issue or if the same or materially similar conduct is already known to the US government);
- It must be made within a *reasonably prompt* time after discovering the violation; and
- It must be *complete*, disclosing all relevant facts known about the violation – including as to individuals substantially involved in the misconduct at issue.

In order to receive credit for a voluntary disclosure, most regulators also require that companies fully cooperate in related investigations, as well as timely and appropriately remediate.

DURING AN ONGOING INVESTIGATION

What are the key characteristics, requirements and best-practice considerations that need to be understood whilst an investigation is ongoing?

The use of technology to gather evidence

US investigations frequently involve the use of technology to forensically preserve, collect, process, and review evidence. For some data sources, such as smart devices and proprietary software, specialised technology must be used to maintain the integrity of the data and to make it available in a useable format for review. US authorities often expect – or require – that productions comply with specific forensic protocols, such as producing metadata.

Privileged communications with counsel

To maximise the application of the US attorney-client privilege in an investigation, best practices include:

- Structuring the investigation so that it is directed by counsel in order to provide legal advice to the client, and documenting this at the outset;
- Keeping privileged communications confidential, such as by limiting dissemination to a defined subset of employees who are part of the investigation team; and
- Marking communications as privileged and confidential, while segregating them from files maintained in the normal course of business.

Interviewing employees and third-party contractors

Attorney interviews of employees can be protected by the attorney-client privilege. It is standard practice for an attorney conducting an investigative interview of a company employee to provide an Upjohn[34] instruction at the outset. This instruction makes clear that:

- The attorney only represents the company and not the individual;
- The interview is being conducted to provide legal advice to the company and as such is protected by the attorney-client privilege; and
- The company alone can decide in its sole discretion whether or not to disclose the substance of the interview to third parties, such as government authorities.

Interviews with third-party contractors are generally not protected by the attorney-client privilege. For this reason, special care should be taken when crafting communications to third parties during an investigation, performing related audits, and conducting interviews of third-party personnel.

In addition to the attorney-client privilege, materials prepared in anticipation of litigation may be protected by the work product doctrine.

Privilege protections for third-party consultants

While the attorney-client privilege generally does not extend to communications with third parties, there

is an exception in some situations when an attorney retains a third-party consultant to assist with a privileged investigation. It is best practice to document this type of retention in what is commonly referred to as a *Kovel*[35] agreement, which specifies that the consultant is being retained to assist with the privileged investigation using its specialised expertise so that the attorney can in turn provide more informed legal advice to the client.

ENFORCEMENT AND PENALTIES

Does the US publicise settlements and judgments?

Generally, yes, each of the civil and criminal regulators of these authorities publicises its enforcement actions. In certain cases, the regulators can even publish decisions not to pursue enforcement actions.

For example, DOJ routinely publicises its settlement of FCPA investigations by deferred prosecution agreement, non-prosecution agreement, or plea agreement – typically accompanied by a DOJ press release. It is even DOJ's current policy to publicise *declinations* awarded in FCPA matters.[36]

On the civil side, SEC, OFAC, BIS, DDTC, and FinCEN all maintain a range of enforcement options that vary from private no action letters, to non-public warning letters, to public fines or other enforcement actions.

Judgments issued by federal courts are generally a matter of public record, as are those by certain administrative tribunals.

Is the use of a deferred prosecution agreement ('DPA') established practice?

Yes. DOJ has been using deferred prosecution agreements to resolve corporate offences for decades. The SEC joined suit in 2011 when it announced its first use of a DPA in a matter involving alleged corporate FCPA offences.[37]

Are administrative/criminal remedies provided for?

Violations of US sanctions, export control, anti-corruption, and AML laws can result in severe civil and criminal penalties. In addition, there may be collateral consequences from such violations, such as debarment, loss of export privileges, licensing revocation, and ancillary litigation from shareholders, victims, and counter parties.

Recent case law, settlements or prosecutions

US enforcement authorities aim to set the global standard for enforcement, often serving as the most active public enforcement body globally across anti-bribery and anti-corruption, export controls, and economic sanctions matters. In a typical year, US authorities will publicly announce dozens of civil and criminal enforcement actions across each of these regulatory areas. For example, in 2020, while OFAC was relatively quiet with 16 settlements for a comparatively limited aggregate $23 million, the DOJ and SEC settled 14 FCPA-related settlements for a record total of an aggregate $6.4 billion.

While each case is fact-specific, a few themes have emerged from recent US enforcement trends, including that authorities will not only (1) focus on companies both big (Airbus (DDTC and FCPA), Amazon (OFAC), and Goldman Sachs (FCPA)) and small (Park Strategies (OFAC) and Broad Tech Systems (BIS)), but also (2) bring enforcement actions against both US (Berkshire Hathaway (OFAC), Alexion Pharmaceuticals (FCPA)) and non-US (Deutsche Bank (OFAC), Nordic Maritime (BIS), Novartis (FCPA)) companies; all companies named were identified in enforcement actions in 2020 alone.

DRAWING TO A CLOSE

How should findings of an investigation be presented?

Investigation findings may need to be presented to a variety of stakeholders, including company personnel, the board of directors, external auditors, and investigating authorities. Common elements of such a presentation include the objectives and scope of the review, the investigative procedures undertaken, the facts identified, and related remedial measures proposed or implemented. Depending on the audience, privileged materials may need to be excluded from the presentation to avoid waivers.

What are the possible outcomes of an investigation?

There are several potential outcomes in US investigations depending on the government authorities involved and nature of the violation at issue. Some of the more common forms of resolution are as follows:

- **Investigation closure letter** – In some (but not all) cases, the investigating agency may provide a letter confirming that its investigation has been closed without an enforcement action against the company. These letters typically state that the investigation may be reopened if new facts are discovered. OFAC, for example, has indicated that in cases where an entity is aware of an investigation, it will issue a formal 'No Action' letter.[38]
- **Warning letter** – One step up from a 'No Action' response is a warning or cautionary letter. These responses are also typically non-public and are issued by an agency where it either determines (a) that there is insufficient evidence of a violation or (b) that the facts do not

warrant a public enforcement response. In such cases the agency will issue a 'Cautionary Letter' (OFAC's term)[39] or a 'Warning Letter' (BIS and FinCEN term).[40]

- **Finding of violation** – One step up from this, OFAC utilises an enforcement tool known as a 'Finding of Violation' in which it publicly identifies a potential violation and the underlying facts, but based on the facts of the case, elects not to pursue a civil fine or penalty.[41]
- **Declination** – DOJ can decide not to pursue an otherwise prosecutable charge via a declination letter. These letters are typically issued issued due to a company's voluntary self-disclosure, cooperation, and remediation – with conditions. For example, in order for DOJ to issue a declination under its FCPA Corporate Enforcement Policy, the company must agree to pay all disgorgement, forfeiture, and/or restitution resulting from the misconduct at issue. In contrast to OFAC or BIS warning letters, DOJ's declinations can be public.
- **Civil penalties** – The civil regulators all maintain authority to pursue civil penalties for violations of their regulations, which, as discussed above, are imposed on a per-transaction basis and can therefore be quite substantial.
- **Non-financial penalties** – The agencies have authority to issue a number of non-financial penalties as well. For example, both BIS and DDTC can issue a denial of export privileges, cutting an entity, or individuals within the entity, off from the ability to access controlled product.[42] OFAC and FinCEN can issue a cease and desist order and/or injunction to require termination of certain conduct.[43] BIS, OFAC, and DDTC can also revoke or modify existing licences.[44]
- **Deferred prosecution agreement ('DPA') / non-prosecution agreement ('NPA')** – These negotiated resolutions are frequently used by DOJ and SEC. DPAs are filed in federal court along with a charging document, and the charges are dismissed after the DPA's requirements are fulfilled. NPAs are not filed with a court.
- **Plea agreement** – In criminal cases, DOJ and a defendant may enter into a plea agreement in which the defendant agrees to plead guilty or no contest to certain charges. In exchange, DOJ may drop or reduce certain charges, or recommend a specific sentence.
- **Civil or criminal complaints** – If the parties cannot agree on a resolution to settle the matter, the investigatory authority typically has one or more judicial or administrative options for commencing a formal adversarial proceeding.

POTENTIAL CONFLICTS OF LAW

Please draw attention to any potential conflicts of law that may arise.

There are a number of conflicts that arise, both because of intentional actions by other countries to limit the perceived extraterritoriality of US law, as well as practical conflicts that can arise in attempting to investigate potential violations of US law in a way that complies with local requirements.

First, and most obviously, investigators need to consider the potential issues raised by 'blocking' statutes maintained by certain countries that prohibit their companies from complying with some, or all, of relevant US law. For example, the European Union has maintained its 'blocking statute' for more than two decades, focused initially on US Cuban sanctions, and updated in 2018 to also capture US 'secondary'

sanctions on Iran.[45] Canada maintains a similar law focused only on US Cuban sanctions, while China has recently passed legislation crafted more broadly to target the 'unjustified extraterritorial application' of unnamed foreign legislation. If an investigation (a) requires operating in a jurisdiction that maintains a relevant 'blocking' statute and (b) involves the statutes covered by that 'blocking' statute, investigators will need to carefully consider how to balance the potentially competing obligations. Doing so typically requires working closely with local counsel in the jurisdiction to design an approach that focuses on permissible areas (e.g., fact gathering, review of compliance with corporate policies, not extraterritorial legislation, etc.) and lays out strict guardrails to avoid lines of inquiry that could create local compliance challenges for the company, investigators, or witnesses.

Second, the inherently global nature of most reviews of US export control, sanctions, FCPA, or AML violations can often generate substantial conflict with local data privacy requirements in the jurisdictions at issue. This section is not intended to fully cover data privacy requirements, but just notes how frequently they can come up in the scope of a global investigation of compliance with US rules. For example, an early step in many investigations – particularly investigations where there is evidence of potentially intentional or wilful misconduct – is to review the correspondence of the parties at issue. However, depending on where those parties (or the data associated with those parties) is located, the investigators may be required to seek consent from the party involved, which may be difficult to obtain or may undermine the relationship with a potential witness.

Worse, some countries maintain criminal blocking statutes, such as China's International Criminal Judicial Assistance law, which regulates the provision of evidence or assistance to foreign countries in connection with criminal proceedings.

While these conflicts can create substantial compliance headaches, they do not automatically result in leniency from the US regulators, which typically approach any claim of a conflict with a sceptical eye. For example, DOJ has expressly stated in several of its enforcement policies that where a company claims that disclosure of overseas documents is prohibited due to data privacy, blocking statutes, or other reasons under foreign law, the company will bear the burden of establishing that prohibition to receive credit for full cooperation.

Links and Notes

1 22 USC. 2778.
2 50 USC. 4801 et seq.
3 50 USC. 1705.
4 50 USC. 4303.
5 15 USC. §§ 78dd-1, 78dd-2, 78dd-3 and 15 USC. § 78m(b).
6 CFTC Division of Enforcement Issues Advisory on Violations of the Commodity Exchange Act Involving Foreign Corrupt Practices, available at https://www.cftc.gov/PressRoom/PressReleases/7884-19.
7 CFTC Orders Vitol Inc. to Pay $95.7 Million for Corruption-Based Fraud and Attempted Manipulation, available at https://www.cftc.gov/PressRoom/PressReleases/8326-20.
8 31 USC. § 5311 et seq.
9 31 C.F.R. § 501.601.
10 Id.
11 15 C.F.R. §§ 762.2(a) & 772.
12 15 C.F.R. § 762.6(a).
13 15 USC. § 78m(b)(2)(A).
14 31 C.F.R. § 1010.410.
15 31 C.F.R. § 1010.430(d).
16 31 C.F.R. § 1020.210(a)(2)(iii) (identifying the requirement for banks; a similar requirement is included in other FinCEN regulations for other AML-regulated entities).
17 22 C.F.R. § 120.25.
18 See OFAC, A Framework for OFAC Compliance Commitments (May 2019), available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf (Hereinafter "OFAC Compliance Framework").
19 USS.G. 8C2.5(f)(3)(C)(i).
20 USAM 9-28.300, 9-28.800. In addition, the US Sentencing Guidelines take into account whether a company had an effective compliance programme in place at the time of the misconduct when calculating the associated criminal fine. USS.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). DOJ's Criminal Division published detailed guidance on how it evaluates corporate compliance programmes. See US Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs, updated June 2020, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.
21 2001 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decision, available at https://www.sec.gov/litigation/investreport/34-44969.htm.
22 https://www.law.cornell.edu/cfr/text/15/appendix-Supplement_No_1_to_part_766
23 31 C.F.R. Part 501, Appendix A ('OFAC Enforcement Guidelines'); and OFAC Compliance Framework.
24 31 C.F.R. §§501.601, 501.602.
25 See e.g., 31 C.F.R. § 1020.320 (obligation for banks).
26 See e.g., 48 C.F.R. §§ 52.203-13(b)(3)(i)(A)-(B) (requiring disclosure when a contractor has 'credible evidence' of certain violations to the Office of the Inspector General, with a copy to the contracting officer, when in connection with the award or performance of a government contract).
27 22 C.F.R. 126.1(e)(2).
28 USS.G. § 8C2.5(g)(1).
29 OFAC Enforcement Guidelines.
30 2001 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decision, available at https://www.sec.gov/litigation/investreport/34-44969.htm.
31 15 C.F.R. § 764.5
32 22 C.F.R. § 127.12.
33 See FinCEN, Financial Crimes Enforcement Network ('FinCEN') Statement on Enforcement of the Bank Secrecy Act (Aug. 18, 2020), available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf (hereinafter 'FinCEN Enforcement Statement').
34 The Upjohn instruction stems from the Supreme Court case *Upjohn v. United States*, 449 US 383 (1981).
35 *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
36 DOJ's FCPA declinations are available here: https://www.justice.gov/criminal-fraud/corporate-enforcement-policy/declinations.
37 Tenaris to Pay $5.4 Million in SEC's First-Ever Deferred Prosecution Agreement, available at https://www.sec.gov/news/press/2011/2011-112.htm.
38 OFAC Enforcement Guidelines, at II(A). See also FinCEN Enforcement Statement, at 2.
39 Id. at II(C).
40 15 C.F.R. Part 766, Appendix, at II(B) ('BIS Enforcement Guidelines'); FinCEN Enforcement Statement, at 2.
41 OFAC Enforcement Guidelines, at II(D).
42 IS Enforcement Guidelines, at II(F); 22 C.F.R. § 127.7.
43 OFAC Enforcement Guidelines, at II(G)(2); FinCEN Enforcement Statement, at 2.
44 OFAC Enforcement Guidelines, at II(G)(2)); BIS Enforcement Guidelines, at II(F).
45 Council Regulation (EC) No 2271/96 (as amended).

This is an extract from
MANAGING INVESTIGATIONS

First published 2021 in the United Kingdom.

A catalogue record for this book is available from the British Library.

ISBN: 978-0-9934917-9-5

Published by D.C. Houghton Ltd.
Editor: Tom Blass
Publisher: Mark Cusick

For more copies of this book, please email info@worldecr.com
Tel: +44 (0) 7702289830

Printed in Great Britain by Encompass Print Solutions
www.encompassprint.co.uk

Correspondence address:
D.C. Houghton Ltd,
Suite 17271,
20-22 Wenlock Road,
London N1 7GU,
England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road,
London N1 7GU, England, UK