Chapter II:
Responding to Requests From Authorities

Summary

Types of Requests

Compulsory Requests: Certain governmental requests are mandatory and enforceable by the relevant government agencies or a court. Such compulsory requests come in a variety of forms, including:

— Grand jury subpoenas;

— Administrative subpoenas;

— Search warrants;

— Financial industry regulatory requests; and

— State-level subpoenas.

Requests for Voluntary Disclosure: Other requests are non-compulsory and the receiving party is not legally required to comply, but may nonetheless determine that it is in its best interest to do so. If not satisfied, such requests sometimes are followed by compulsory requests.

Early Considerations

Upon receiving a compulsory or voluntary request, and throughout the investigation that follows, a company should consider certain issues, including:

— The nature and purpose of the investigation;

— Whether to seek to quash or modify a subpoena, or negotiate the scope of a request;

— Document retention;

— Legal limitations on data dissemination;

— The potential impact of decisions regarding production in response to one request on the company's ability to produce or withhold from production in response to requests from other jurisdictions; and

— Providing a timely and effective response in a way to minimize the chance for follow-on requests.

Introduction

In some instances, early strategic decisions concerning how to respond to a request for information can effectively work to limit, or at a minimum, frame the scope of additional inquiry. However, responses need to be carefully crafted to ensure that requesting authorities do not get the misimpression that a recipient is wary of fully complying or is hiding something. In addition, the sheer number of regulatory and criminal agencies, their varying powers to compel production, and their own internal practices and cultures further complicate what are generally the twin goals of responding to a request: (i) to get the requesting authority what it needs as efficiently as possible while maintaining credibility, and (ii) to appropriately cabin the scope of inquiry to the relevant subject matter to minimize the burden. In addition, there are important practical considerations that are best reviewed at the outset of receiving a request for information and kept in mind while responding, in order to protect privileged and other confidential information and to help ensure that the investigation progresses smoothly. This chapter discusses some of the different types of compulsory and voluntary requests a company may receive, discussing practices of specific agencies as examples only, as well as potential issues and strategies that should be considered in order to respond effectively.

Compulsory Requests for Information[1]

Grand Jury Subpoenas

In the United States, the grand jury's purpose is to determine whether charges against a suspect are warranted. The grand jury does not sit to determine guilt or innocence, but rather, to assess whether there is a basis to bring a criminal charge.[2] Accordingly, grand jury subpoenas are a compulsory process used by criminal prosecutors to pursue an investigation, through which the grand jury determines whether there is probable cause to believe a crime has been committed. As such, the grand jury is not required to make a preliminary showing of probable cause

[1] It is important to keep in mind, however, that there are many more criminal and regulatory authorities, both in the United States and elsewhere, and companies should consider the particular practices of each relevant authority on a case-by-case basis.

[2] *See* U.S. Const. amend. V ("No person shall be held to answer for a capital, or otherwise infamous [federal] crime, unless on a presentment or indictment of a Grand Jury").

before initiating an investigation, and a grand jury subpoena can be issued based on mere suspicion that the law is being violated or to seek assurance that it is not.[3]

Grand jury subpoenas have a substantially broader reach than subpoenas used in criminal or civil litigation, where the specific offense or conduct at issue has already been identified. In the absence of a probable cause requirement, the grand jury is empowered to issue broad requests for witness testimony (through a *subpoena ad testificandum*), as well as for documents, papers, and other physical evidence (through a *subpoena duces tecum*), which may include confidential information.[4] Notably, grand jury proceedings are conducted in virtually complete secrecy pursuant to the Federal Rules of Criminal Procedure and comparable state laws.[5]

Failure to comply with a grand jury subpoena may constitute civil or even criminal contempt.[6] Nevertheless, the grand jury's authority is not self-executing and it must rely on the courts to enforce a contempt order.[7] A party subject to a grand jury subpoena may seek to limit the subpoena's reach by moving to quash or modify the subpoena before a court; however, the court's ability to quash a grand jury subpoena is limited by a high standard of reasonableness, and the burden frequently is on the moving party to demonstrate that the request is unreasonable.[8] Courts may also quash or modify a grand jury subpoena on grounds that the materials or testimony sought are protected by a valid, recognized privilege, that the subpoena will infringe upon a constitutional right, or that the government has abused the grand jury process.[9] Abuse of the grand jury process occurs, for example, where a subpoena is used improperly to obtain information for a parallel civil litigation.[10]

---

[3] *United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991) (defining a grand jury as "an investigatory body charged with the responsibility of determining whether or not a crime has been committed").

[4] Fed. R. Crim. P. 17(c).

[5] Fed. R. Crim. P. 6(e)(2)(B).

[6] Fed. R. Crim. P. 17(g).

[7] *Id*. *See also United States v. Williams*, 504 U.S. 36, 48 (1992) ("[T]he grand jury cannot compel the appearance of witnesses and the production of evidence, and must appeal to the court when such compulsion is required.").

[8] *See R. Enters., Inc.*, 498 U.S. at 301("[A] grand jury subpoena issued through normal channels is presumed to be reasonable, and the burden of showing unreasonableness must be on the recipient who seeks to avoid compliance.").

[9] *See, e.g., Williams*, 504 U.S. at 48 ("[T]he court will refuse to lend its assistance when the compulsion the grand jury seeks would override rights accorded by the Constitution . . . or even testimonial privileges recognized by the common law.").

[10] *See, e.g., United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958) ("[The] 'indispensable secrecy of grand jury proceedings,' must not be broken except where there is a compelling necessity.")(citation omitted).

Administrative Subpoenas[11]

Subpoenas served by administrative agencies—for example, the U.S. Securities and Exchange Commission ("SEC" or "Commission"), the Office of Foreign Asset Control ("OFAC"), or the Department of Labor ("DOL"), among others—may serve a variety of purposes, including gathering information to issue future rules or regulations,[12] or to investigate and formally adjudicate suspected misconduct. Administrative subpoena power is derived from agency enabling statutes and regulations and can impart broad investigative authority on the relevant agency. Like grand jury subpoenas, administrative subpoenas generally do not require a showing of probable cause prior to issuance, and can be issued based "merely on suspicion that the law is being violated, or even just because [the agency] wants assurance that it is not."[13] Thus, administrative subpoenas often serve as powerful tools that enable U.S. government agencies to undertake broad investigations.

Notwithstanding the broad reach of administrative subpoenas, some caveats limit their power. For example, administrative subpoenas are subject to constitutional and jurisdictional limitations. Although the Supreme Court has sanctioned the broad investigatory powers of administrative agencies,[14] administrative subpoenas are still subject to the reasonableness standards of the Fourth Amendment, and will be found to comply "so long as it is 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'"[15] Likewise, agency enabling statutes apply jurisdictional limitations on the scope of an agency investigation.[16]

---

[11] Due to the wide variety of regulatory agencies, this chapter contains a general discussion of administrative subpoenas and some generally applicable considerations.

[12] *See, e.g., F.T.C. v. Brigadier Indus. Corp.*, 613 F.2d 1110 (D.C. Cir. 1979) (discussing the Federal Trade Commission's authority to issue subpoenas as part of its rule-making process).

[13] *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950); *see also United States v. Powell*, 379 U.S. 48, 51-53 (1964) (discussing absence of a probable cause requirement).

[14] *See, e.g., Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209, 214 (1946) (acknowledging the broad investigatory powers Congress may delegate to administrative agencies and that such "authority would seem clearly to be comprehended in the 'necessary and proper clause'").

[15] *Carpenter v. United States*, 585 U.S. ____, (2018) (Kennedy, J. dissenting) (quoting *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984)); *see also C. A. B. v. United Airlines, Inc.*, 542 F.2d 394, 395 (7th Cir. 1976) (refusing to enforce a subpoena when the administrative agency would not specify its investigative purpose or make its demand reasonably definite).

[16] *See United States v. Holstrom*, 242 F. App'x 397, 398 (9th Cir. 2007) (dismissing an indictment when the agency's enabling statute did not provide authority for such investigatory powers over the rail service).

Further, even where an agency has legal authority to issue a subpoena, agency staff may be required to obtain written authorization from senior officers within the agency before they can issue subpoenas, which can be a somewhat time-consuming process.[17] In addition, administrative subpoenas are not self-enforcing. Failure to comply with an administrative subpoena, standing alone, typically does not constitute contempt or expose the recipient to sanctions absent a court order. If a subpoenaed party fails to comply with a federal agency's request, the agency must petition the relevant federal district court to compel compliance.[18] The district court's ruling either for or against enforcement of the subpoena constitutes a final, appealable decision, and a subpoena recipient who violated that court order could be subject to a civil, or even criminal, contempt charge.[19]

When an agency seeks judicial enforcement of an administrative subpoena, courts will consider whether the agency can show "that the investigation will be conducted pursuant to a legitimate purpose, that the inquiry may be relevant to the purpose, that the information sought is not already within the [agency's] possession, and that the administrative steps required . . . have been followed."[20] Courts may refuse to enforce an agency subpoena, for example, where it can be shown that the subpoena was intended to harass or is unduly burdensome to the recipient.[21] At the time of judicial enforcement, the recipient can challenge the administrative subpoena, and bears the burden of demonstrating that it is invalid. This is a high bar, however, as courts typically do not permit discovery into agency motives for instituting an investigation unless the recipient is able to demonstrate facts indicating abuse.[22]

Thus, the non-self-enforcing nature of administrative subpoenas presents strategic considerations regarding the extent to which a company may choose to comply

[17] For example, SEC staff must receive a formal order of investigation—authorized by either the Commission itself or the Director of the Division of Enforcement—to issue subpoenas compelling testimony and the production of documents. The order describes the general nature of the investigation and identifies provisions of the federal securities laws that may have been violated. *See* 15 U.S.C. § 78u(a)-(b) (2018); *How Investigations Work*, Sec. Exch. Comm'n, https://www.sec.gov/enforce/how-investigations-work.html (last visited July 25, 2018).

[18] *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 741 (1984) ("Subpoenas issued by the Commission are not self-enforcing, and the recipients thereof are not subject to penalty for refusal to obey. But the Commission is authorized to bring suit in federal court to compel compliance with its process.").

[19] *See* 5 U.S.C. § 555 (d) (2018).

[20] *Powell*, 379 U.S. at 57-58.

[21] *Id*. U.S. at 58 ("Such an abuse would take place if the summons had been issued for an improper purpose, such as to harass . . . or to put pressure . . . to settle a collateral dispute, or for any other purpose reflecting on the good faith of the particular investigation.").

[22] *See, e.g., id.*; *United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 316-17 (1978); *United States v. Judicial Watch, Inc.*, 241 F. Supp. 2d 15, 17 (D.D.C. 2003).

at the outset. On one hand, there may be latitude for recipients to negotiate an administrative subpoena's scope, as agency staff may be willing to work with recipients rather than expending the agency's time and resources to seek judicial enforcement. On the other hand, given the broad investigative authority and great deference afforded to federal agencies by courts, refusal to comply with an agency subpoena may only serve to delay the investigation and potentially antagonize the requesting agency.

State-Level Subpoenas

State-level administrative and civil subpoenas, which vary by state, are utilized by authorities at the state level to require the production of certain documents or information. In New York, for example, the Department of Financial Services ("DFS") has statutory authority to "subpoena witnesses, to compel their attendance, to administer an oath, to examine any person under oath and to require the production of relevant books or papers."[23] The New York Attorney General's Office ("NYAG"), which has general authority to conduct investigations into securities or commodities fraud and to bring civil and criminal actions, also has broad power to issue subpoenas statewide to compel the appearance of witnesses or the production of documents in connection with an investigation under the Martin Act.[24] Failure to comply with a DFS or NYAG subpoena constitutes a misdemeanor.[25]

Other Compulsory Requests

Civil Investigative Demands

An increasingly common form of compulsion is the Civil Investigative Demand ("CID"), which is used to obtain documentary information, answers to interrogatories, and oral testimony when there is reason to believe that a party has engaged in certain misconduct or wrongdoing. CIDs, which are authorized by statute, are typically quite broad in scope, and permit the federal government to investigate and determine whether there is sufficient evidence to justify the expense

[23] N.Y. Banking Law § 38 (2018).

[24] It is widely recognized that the powers granted to the New York Attorney General under the Martin Act are very broad. *See Anwar v. Fairfield Greenwich Ltd.*, 728 F. Supp. 2d 354, 367 (S.D.N.Y. 2010) (describing the Martin Act as "a statute of enormous breadth and unique dimensions.") (quoting *D'Addio v. L.F. Rothschild. Inc.*, 697 F. Supp. 698, 707 (S.D.N.Y.1988)); *see also* N.Y. Gen. Bus. Law § 352(2) (2018) (The Martin Act).

[25] N.Y. Gen. Bus. Law § 352(4) (2018); N.Y. Banking Law § 38 (2018).

of pursuing litigation. For example, the Department of Justice ("DOJ") may issue CIDs where the government is investigating antitrust violations, False Claims Act ("FCA") violations, or civil racketeering.[26] Financial industry regulators, such as the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB"), may also have authority to issue CIDs seeking documents, responses to interrogatories, tangible items, or deposition testimony.[27]

National Security Letters

National security letters ("NSLs") allow the Federal Bureau of Investigation ("FBI") to gather information for purposes of national security. Authorizing statutes specify the type of information that may be sought via NSL, including subscriber information and toll billing records, consumer identifying information, and financial records.[28] The FBI can issue NSLs without obtaining prior approval from a judge,[29] and recipients are often subject to gag orders and prohibited from sharing the fact that they have received an NSL.[30] To challenge an NSL, a recipient may "petition for an order modifying or setting aside the request" in the federal district court where the NSL recipient does business or resides, and the court may modify or set aside the request if it finds that compliance would be "unreasonable, oppressive, or otherwise unlawful."[31] Similarly, the Attorney General must go to the district court in the jurisdiction in which the investigation is taking place or the recipient resides, does business, or may be found, to compel compliance.[32]

[26] *See* 15 U.S.C. § 1312 (2018) (antitrust); 31 U.S.C. § 3733 (2018) (false claims); 18 U.S.C. § 1968 (2018) (racketeering).

[27] *See* 15 U.S.C. § 57b-1 (2018) (FTC); 12 U.S.C. § 5562 (2018) (CFPB).

[28] The FBI's authority to issue NSLs is derived from several statutes, including: the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2018) (government permitted to request subscriber information and toll billing records); the Fair Credit Reporting Act, 15 U.S.C. § 1681u (2018); the Right to Financial Privacy Act, 15 U.S.C. § 1681v (2018) (government permitted to request consumer identifying information); and 12 U.S.C. § 3414 (2018) (government permitted to request financial records).

[29] 12 U.S.C. § 3414(a)(5) (2018).

[30] *See, e.g.*, 18 U.S.C. § 2709(c)(1) (2018).

[31] 18 U.S.C. § 3511(a) (2018).

[32] 18 U.S.C. § 3511(c) (2018).

Search Warrants

In addition to grand jury and administrative subpoenas, criminal authorities may use search warrants as tools to seize physical and electronic evidence. Search warrants are written orders issued by a federal district or magistrate judge directing law enforcement agencies to search specific premises and to seize specific persons or property.[33] The warrant must specify the person or property to be searched or seized.[34] Unlike grand jury or administrative subpoenas, the district or magistrate judge must find probable cause that a crime has been committed before issuing a warrant.[35] In addition, unlike subpoenas, which typically afford recipients time to respond, search warrants authorize law enforcement and government agencies to immediately seize the evidence they are seeking. Whereas a subpoena can be quashed in certain circumstances or must otherwise be enforced, a company often has no legal recourse to prevent the execution of a search warrant and, in most cases, a challenge can only be made after the fact,[36] typically in the form of a pre-trial motion to suppress and/or a motion for return of property.[37]

Financial Industry Regulatory Requests

Outside of subpoenas and warrants, there are a number of financial industry regulatory or self-regulatory agencies that have authority to issue compulsory

[33] Fed. R. Crim. P. 41(b).

[34] Fed. R. Crim. P. 41(e)(2)(A).

[35] Fed. R. Crim. P. 41(d)(1).

[36] *See Dalia v. United States*, 441 U.S. 238, 239 (1979) ("[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness."). It is worth noting that there may be limited occasions where companies can resist and successfully challenge government warrants in certain contexts. For example, the Stored Communications Act ("SCA"), which provides that the government can issue a warrant for service providers to provide certain customer information, contains a mechanism by which service providers can challenge or move to quash such warrants. 18 U.S.C. § 2703(d) (2018). The ability of the United States government to compel data stored abroad pursuant to the SCA was recently clarified through the introduction of the Clarifying Lawful Overseas Use of Data ("CLOUD") Act, which provides a mechanism for service providers to challenge or move to quash warrants issued pursuant to SCA, seeking disclosure of electronic communications stored exclusively on servers at datacenters abroad. *See* CLOUD Act § 103(a)(1), codified at 18 U.S.C. § 2713 (2018). By introducing a procedure for pre-enforcement challenges to SCA warrants, the CLOUD Act effectively aligns such warrants with the procedures for enforcing subpoenas, discussed above.

[37] Under Federal Rule of Criminal Procedure 41(g), a "person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). Rule 41(h) likewise allows a defendant to move to suppress evidence. In a recent and highly publicized example, in April 2018, the FBI executed broad search warrants for President Trump's former lawyer and associate Michael Cohen's residence, hotel room, office, safety deposit box, and electronic devices. Although Mr. Cohen could not prevent the execution of the warrant, his counsel immediately requested that the seized materials be returned to Mr. Cohen's counsel for initial review and production, and then moved for a temporary restraining order to prevent the government from reviewing the materials. In the Southern District of New York, the Court ultimately resolved the issue by appointing a special master to review the documents for privilege. *See* Order of Appointment, *Michael Cohen v. United States*, No. 18-mj-03161 (S.D.N.Y. Apr. 27, 2018), ECF No. 30.

requests to entities that fall within their regulatory ambit.[38] Self-regulatory organizations ("SROs"), for example, supplement the SEC's regulatory authority.[39] The SEC delegates to SROs the ability to regulate their members, including authority to discipline, expel, and suspend members for conduct "inconsistent with just and equitable principles of trade."[40] One of the more notable SROs is FINRA, which regulates the broker-dealer community, and has authority to investigate conduct that violates the securities rules through discovery requests for documents and information, as well as authority to fine, suspend, or bar broker-dealers who do not comply.[41] There are a host of other SROs in addition to FINRA, including, for example, the New York Stock Exchange ("NYSE"), which have authority similar to FINRA's over their members.[42] The SEC has supervisory authority over FINRA and other SROs, and may abrogate or change their rules.[43] To challenge a FINRA request, the recipient must refuse compliance and appeal any disciplinary action to the SEC.[44]

It should be noted that SROs' power over their members is generally very broad. For example, FINRA and the NYSE have taken the position that merely refusing to produce documents in response to a request or appear for testimony constitute violations of their rules that can, standing alone, result in disciplinary proceedings, resulting in fines, bars, or other sanctions, irrespective of whether a substantive violation of the securities laws can be shown.

---

[38] Relevant financial industry regulatory agencies include the SEC, the Financial Industry Regulatory Authority ("FINRA"), the Federal Reserve Bank (the "Fed"), the Commodity Futures Trading Commission ("CFTC"), the FTC, the CFPB, and the Office of the Comptroller of the Currency ("OCC"), among others.

[39] SROs are non-governmental organizations authorized by Congress to create and enforce industry regulations and standards. *See* Section 10B(c) of the Securities Exchange Act of 1934.

[40] 15 U.S.C. § 78f (2018).

[41] FINRA Rule 8210 grants FINRA authority to inspect and copy books, records, and accounts of member firms. *See Information and Testimony Requests*, Fin. Industry Reg. Auth., http://www.finra.org/industry/information-and-testimony-requests (last visited Aug. 1, 2018); *What We Do*, Fin. Industry Reg. Auth., https://www.finra.org/about/what-we-do (last visited Aug. 1, 2018).

[42] NYSE Regulation ("NYSER") is responsible for monitoring activities on the NYSE's exchanges, and for addressing non-compliance by NYSE members with the NYSE's rule and the applicable federal securities laws. While some regulatory functions are performed directly by NYSER, others are performed by FINRA or another self-regulatory organizations pursuant to a regulatory service agreement. Disciplinary Actions stem from a variety of sources, such as internal referrals, investor complaints, examinations of member organizations, and referrals from the SEC. *See NYSE Regulation*, New York Stock Exch., https://www.nyse.com/regulation (last visited July 25, 2018).

[43] *See* 15 U.S.C. § 78s(b)(7)(C) (2018).

[44] *See In re Application of Jay Alan Ochanpaugh*, No. 3-12147, 2006 SEC LEXIS 1926, at *21 (Sec. Exch. Comm'n Aug. 25, 2006).

PRACTICE TIP: CONSIDERATIONS OF INTERNATIONAL FINANCIAL INSTITUTIONS AND DEVELOPMENT ORGANIZATIONS

In addition to requests from U.S. government regulators, international financial institutions and development organizations, such as the World Bank Group (the "World Bank"), may also make requests or solicit information, particularly through contractual audit rights.[45] Although the World Bank does not have formal subpoena power, failure to comply with a request may nevertheless constitute a sanctionable offense with broad commercial consequences.[46]

— The World Bank can issue a Notice of Temporary Suspension, temporarily suspending a respondent from entering into new contracts with the World Bank,[47] but it can also initiate more formal proceedings with a wide range of possible sanctions:

- **Reprimand:** The sanctioned party is formally reprimanded;[48]
- **Conditional Non-Debarment:** The sanctioned party is required to comply with certain remedial, preventative, or other conditions in order to avoid debarment from World Bank Projects;[49]
- **Debarment:** The sanctioned party is declared ineligible (either indefinitely or for a specified period of time) from benefiting from participation in certain Bank-financed contracts or projects.[50]
- **Debarment with Conditional Release:** The sanctioned party is only released from debarment if it demonstrates compliance with certain remedial, preventative, or other conditions for release, after a specified period of debarment.[51]
- **Restitution:** The sanctioned party must pay restitution to remedy the harm caused by its misconduct.[52]

[45] World Bank Grp., *The World Bank Group's Sanctions Regime: Information Note12* (Nov. 2011), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/The_World_Bank_Group_Sanctions_Regime.pdf..

[46] World Bank Grp., *World Bank Group Sanctions Procedures*, Appendix 1 (Apr. 2012), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/WBGSanctions_Procedures_April2012_Final.pdf.

[47] *Id*. at Article II, § 2.01.

[48] *Id*. at Article IX § 9.01(a).

[49] *Id*. at Article IX § 9.01(b).

[50] *Id*. at Article IX § 9.01(c).

[51] *Id*. at Article IX § 9.01(d).

[52] *Id*. at Article IX § 9.01(e).

— Debarment can be particularly burdensome to companies as it extends to other development banks that have entered into a "cross-debarment agreement" with the World Bank cross acknowledging debarments by other multilateral banks.[53]

— One point to consider is the impact that disclosure to institutions such as the World Bank could have on privilege protections. While privileged materials are considered exempt from disclosure in World Bank sanctions proceedings,[54] if such materials are disclosed it could constitute a privilege waiver.[55]

Responding to Compulsory Requests

PRACTICE TIP:
CHALLENGING OR NEGOTIATING AN ADMINISTRATIVE SUBPOENA—QUESTIONS TO CONSIDER

— Does the requesting agency have jurisdiction?

— Does the scope of the subpoena go beyond the reasonable needs of the investigation?

— Was the subpoena issued pursuant to a legitimate purpose of the agency, and does it comply with the authority granted through the agency's enabling statute?

— Is the request overly vague or indefinite?

— Was the request made in good faith or for an improper purpose?

— Does the subpoena violate a constitutional right or request privileged information?

[53] These include the Asian Development Bank, African Development Bank, European Bank for Reconstruction and Development, and the Inter-American Development Bank. *See* World Bank Grp., *The World Bank Group's Sanctions Regime: Information Note 9* (Nov. 2011), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/The_World_Bank_Group_Sanctions_Regime.pdf.

[54] World Bank Grp., *World Bank Group Sanctions Procedures*, Article VII § 7.02 (Apr. 2012), http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/WBGSanctions_Procedures_April2012_Final.pdf.

[55] For more information on preserving legal privilege, *see* Chapter [IV]: [Preserving Legal Privilege].

Early Considerations When a Company Receives a Compulsory Request

Upon receipt of a compulsory request for information, counsel and the company should first consider whether the requesting authority has jurisdiction to issue such request, and whether lack of jurisdiction limits the company's obligation to respond. Jurisdictional considerations should be given appropriate weight *before* responding to a request, as an improvident exchange of information with an agency that does not have jurisdiction can result in a waiver of jurisdictional arguments.

Once jurisdiction and other legal authority is established, counsel and the company should consider initiating an early discussion with the issuing authority, to build rapport and better understand the underlying purpose of the request. In addition, counsel and the company should consider whether to request an extension of time to respond, and whether the information requested can be narrowed through negotiations with agency staff. Where counsel has established credibility and demonstrated a willingness to cooperate, authorities may be open to engaging in some discussion in an effort to accelerate their access to relevant information and ultimately expedite their investigation. In addition, in industry-wide investigations, it may be useful to engage in joint-defense discussions with peer institutions who may be further along in the investigation process, to gain additional information before preparing a response.

PRACTICE TIP: EARLY CONSIDERATIONS UPON RECEIPT OF A REQUEST FOR INFORMATION

— **Scope.** Consider whether to discuss the subject matter of the request with the issuing authority to better understand its purpose and explore whether it would be possible to narrow its scope.

— **Timing.** Consider whether the schedule in place for the production of documents and information is reasonable, and whether a request for an extension of time is warranted. In cases where a large volume of information is requested, consider proposing a schedule for partial productions to be made at regular intervals. Because credibility is an important factor, it is usually better to set reasonable and realistic expectations at the outset, rather than running up against deadlines and needing to seek additional time after the fact.

— **Purpose.** Consider the purpose of the investigation and the company's role to determine how best to respond to the request. In particular, it may be helpful to clarify with the issuing authority whether the relevant government agency considers the company a witness, subject, or target.[56]

— **Quash or modify.** Consider whether there may be grounds to quash or modify the subpoena or request, or opportunities to negotiate its scope, as well as whether there are any legal limitations on the data that can be provided in response.

— **Custodians.** Immediately upon receipt of a request for document production, consider which custodians are likely to have relevant information. This is not only necessary to collect and retain relevant documents, but will allow a company to get a leg up on both understanding the scope and subject matter of the request and possibly negotiate for a narrower production.

— **Document retention and custodian of records.** Promptly prepare a litigation hold notice to circulate to employees, as well as a certification for employees to acknowledge compliance, and consider suspending regular document deletion or destruction procedures. It may also be helpful to appoint a custodian of records at the company to liaise with counsel to ensure compliance with the request. Also

[56] The terms "subject" and "target" are commonly used in the criminal context to characterize the role of a company or individual being investigated in contrast to a witness, which is primarily viewed as a source of information rather than a focus of the investigation. The U.S. Attorney's Office Manual defines a "subject" of an investigation as "a person whose conduct is within the scope of the grand jury's investigation," and a "target" as "a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant." Dep't of Just., *U.S. Attorneys' Manual* § 9-11.151 (Nov. 1997) ("USAM"). Some civil agencies—particularly those that often investigate potential misconduct in conjunction with criminal authorities—are also familiar with, and use, this lexicon. While some agencies may not use the same designations, they may nonetheless be willing to discuss the nature of the investigation. The SEC, for example, does not identify "targets" of its investigations; it does, however, issue formal investigation orders which describe the nature of the investigation, and can be requested by a party subject to investigation. *See* Sec. Exch. Comm'n, *Enforcement Manual* §§ 3.3.2, 2.3.4.2 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

consider alerting the company's human resources or information technology department that normal document retention procedures should be suspended and documents should be retained until further notice for departing employees who may have relevant documents.

— **Joint defense.** Consider whether entering into any joint defense agreements—for example, with individual counsel for represented employees or with peer institutions subject to the same investigation—would be useful.

Limitations on Data Dissemination

In the early stages of responding to a compulsory request, companies should consider whether any legal protections might limit their obligation, and indeed their legal ability, to produce the requested information, to avoid inadvertently including such information in a response. Some protections that should be considered at the outset include:

Jurisdictional Limitations

As discussed above, a company should first consider whether there are jurisdictional limitations to the requesting authority's legal ability to issue the request and/or collect certain documents and information. This is often a fact-intensive inquiry, which turns on factors such as the requesting authority's location and jurisdictional authority, the location of the company and its affiliates, and the location of the documents and individuals to be produced.[57] For example, it is not unusual for subpoenas to be served on corporate entities present in the United States, to reach an entity located in another jurisdiction which "owns" the documents sought by the subpoena. Such entity may be a parent company, a subsidiary, or an affiliate with no U.S. presence. Responsibility to produce requested information can turn on whether the domestic affiliate has sufficient control of the responsive overseas documents to render them subject to production in the United States.[58]

[57] It should be expected that agencies will argue that deference should be given to their interpretations of their own jurisdictional limitations, particularly at the investigatory stage. *See F.T.C. v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) ("as a general proposition, agencies should remain free to determine, in the first instance, the scope of their own jurisdiction when issuing investigative subpoenas") (citing *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501 (1943)).

[58] *See In re Canadian Int'l Paper Co.*, 72 F. Supp. 1013, 1020 (S.D.N.Y. 1947) (In grand jury proceedings: "The test [for the production of documents] is control— not location").

Attorney-Client Privilege and Attorney Work-Product

In the United States, attorney-client privilege protects against disclosure of communications between a lawyer and client made for the purpose of seeking or providing legal advice, and extends to communications made during the course of an internal investigation between a company's employees and the company's counsel.[59] The work-product doctrine protects against disclosure of documents (or other tangible items) containing mental impressions, opinions, or legal theories prepared in anticipation of litigation.

The rules regarding privilege and work product differ depending on the jurisdiction whose laws apply, and it will be important to be sensitive to the choice-of-law issues as well as the substantive law of privilege in the relevant jurisdictions. As discussed above, materials covered by either attorney-client privilege or attorney work-product need not be disclosed in response to a compulsory request. However, consideration of these protections at the outset is critical, as they may be inadvertently waived.[60]

Confidential Supervisory Information

Financial institutions supervised by the Board of Governors of the Federal Reserve Bank (the "Board") may have access to confidential supervisory information ("CSI"), which is subject to the Board's regulations governing its disclosure.[61] In practice, CSI covers information related to the examination of a financial institution by a bank examiner.[62] Because all CSI remains the property of the Board, no supervised institution or individual, to whom the information has been made available, may disclose such information without the prior written consent of the Board's general counsel, unless a specified exception applies.[63]

Suspicious Activity Reports

Banks are required to file suspicious activity reports ("SARs") with the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), upon detecting

---

[59] *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).

[60] For a more detailed discussion of legal privilege, *see* Chapter IV: Preserving Legal Privilege.

[61] *See generally* 12 C.F.R. § 261 (2018).

[62] *See* 12 C.F.R. § 261.2(c)(1)(ii)-(iii) (2018). Relevant bank examiners include the Fed, the OCC, DFS, the CFPB, and the Federal Deposit Insurance Corporation ("FDIC"), among others.

[63] *See* 12 C.F.R. § 261.20(g) (2018). Upon request, the Board may make CSI available to federal or state financial institution supervisory agencies, and may authorize other discretionary disclosures of CSI as necessary. *Id.* at § 261.20 (c), (d), (e) (2018).

or suspecting that a crime is taking place.[64] Banks may be required to submit SARs in certain circumstances, or may report suspicious activities voluntarily. In either case, SARs are confidential and may not be disclosed except as specified by statute and in FinCEN's regulations; statutory and regulatory exceptions may allow disclosure of SARs to certain law enforcement and supervisory agencies.[65]

Blocking Statutes or Restrictions on Cross-border Data Transfers

Blocking statutes are enacted by certain jurisdictions to prohibit exporting documents for use in judicial or administrative proceedings without government consent.[66] Data privacy laws similarly restrict cross-border access to information stored in certain countries, particularly in the EU.[67] Even where there is no applicable blocking statute or data privacy law, certain foreign authorities may require that they be notified of a request that implicates data or documents stored in their jurisdiction, and may further require that the information be provided through the local authority as a conduit. For example, the UK Financial Conduct Authority ("FCA") sets forth procedures by which information stored in the UK must be produced pursuant to a Notice of Requirement ("NOR").[68]

It is important to consider the importance of blocking statutes or similar other restrictions at the very beginning of an inquiry before any documents are collected. Decisions with respect to where to view documents and whether to transfer documents from a jurisdiction that has a blocking statute to one that happens not to have such a statute can have dramatic—and sometimes unintended—consequences for a later stage of the investigation when the documents are requested. Companies should, therefore, be mindful of not running afoul of laws restricting cross-border transfers of documents and information, particularly where a company has offices in other jurisdictions. Moreover, such jurisdictional requirements may provide an opportunity to negotiate narrowing the scope of a request, in the interest of obtaining

[64] Fin. Crimes Enforcement Network, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions* 80 (2012), https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf.

[65] *See, e.g.*, 31 U.S.C. § 5318(g) (2018); 31 C.F.R. § 103.18(e) (2018); 12.C.F.R. § 21.11(k) (2018).

[66] 3 Robert L. Haig, *Business and Commercial Litigation in Federal Courts* § 21:97 (4th ed. 2017).

[67] *See* Council Directive 95/46, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31; General Data Protection Regulation (GDPR) 2016/679, 2016 O.J. (L. 119) 1. Data privacy and blocking statutes, including the European Union's recently enacted GDPR, are discussed in further detail in Chapter V: Data Privacy & Blocking Statutes.

[68] *See* Financial Services and Markets Act 2000 §§ 169 (Investigations in support of overseas regulator), 195 (Exercise of power in support of overseas regulator) (Eng.).

approval from the foreign authority to facilitate the production of the information sought by the requesting authority.

Other Confidential Information

In some instances, information that may not be covered by a statutory or other legal doctrine may still be protected from disclosure. For example, in the case of personally identifiable information ("PII"), which can be used to identify an individual in context (for example, name, social security number, passport number, driver's license number, address, or phone number), authorities may be amenable to redaction where the PII would be irrelevant to the purpose of their investigation. In addition, where PII is produced, there may be statutory limitations on further disclosure by the relevant authority,[69] or the authorities themselves might offer procedures by which a company can seek confidential treatment.[70]

Companies may also have entered into confidentiality agreements with clients or customers restricting their ability to disclose certain information. Although standard non-disclosure agreements typically include contractual provisions accounting for the possibility of compulsory requests, they also frequently have notice provisions that must be carefully considered and analyzed before documents are produced. In addition, there may be common law provisions that provide exceptions to confidentiality for government requests. Companies might also consider requesting confidential treatment following the production of such information, to limit further disclosure and any collateral liability under the terms of an applicable contract.[71]

[69] *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2018) (governing disclosure of PII). It should be noted, however, that prohibitions against disclosure may not apply where such disclosure is required by the Freedom of Information Act, or where another federal, state, or local government requests such information for purposes of civil or criminal law enforcement. 5 U.S.C. § 552a(b)(2), (b)(7) (2018).

[70] *See e.g.*, 17 C.F.R. § 200.83 (2018) (setting forth a procedure by which those submitting information to the SEC may request that it not be disclosed pursuant to a request under the Freedom of Information Act).

[71] For example, the SEC Enforcement Division may enter into confidentiality agreements with a company subject to investigation, by which the SEC would agree not to assert privilege waiver as to a third party of documents produced by the company that it would otherwise withhold as privileged. *See* Sec. Exch. Comm'n, *Enforcement Manual* § 4.3.1 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. In addition, the SEC might agree to maintain confidentiality over certain materials provided by a company, "except to the extent that the staff determines that disclosure is required by law or that disclosure would be in furtherance of the SEC's discharge of its duties and responsibilities." *Id*.

Negotiating the Scope of the Request

In addition to working through the practical considerations of responding to a request—identifying the relevant custodians, collecting and retaining relevant documents, and determining whether the request is within the agency's authority—consideration should also be given to negotiating the scope of the request.

Quite often agency requests are broadly drawn. There are numerous reasons for this, including that agency attorneys are often at the beginning of an investigation and wary of missing relevant information. Careful consideration should be given to whether to attempt to negotiate the precise scope of a request at the outset. A discussion about how a request can be narrowed may help the government by assisting it in targeting the documents that will be most relevant to its investigation and imposing on the company (rather than the government) the obligation to separate the "wheat from the chaff." At the same time, a discussion regarding narrowing a request may buy the company needed goodwill from the government, may reduce the costs of document production, and might avert the production of documents that while irrelevant lead to a broadening of the government investigation. Agencies are often amenable to such negotiations because—assuming that responding counsel has credibility and rapport with the agency—they can lever the company's expertise to help focus them on the documents most relevant to their inquiry. Moreover, the company and its counsel typically better understand the industry and are thus often better equipped to provide the most relevant information in the shortest possible time. Finally, from the agency's perspective, there is likewise value in building rapport and trust—it often means that companies will work to provide information beyond the strict limits of the request or, indeed, the agency's subpoena power, for example, by preparing reports, presentations, or interrogatory responses that are both, strictly speaking, beyond many agencies' subpoena power and highly useful in focusing on the most critical evidence. Government attorneys, who often face their own resource limitations, would also like to avoid the proverbial "document dump."

In negotiating the scope of a response, there are a number of considerations to keep in mind:

— ***Establish a dialogue.*** Initiating an early conversation may help to establish an ongoing dialogue with the investigating authority. Establishing an ongoing dialogue at the outset of the investigation helps to set the stage for negotiating the scope of the request, while keeping the door open for further negotiations down the road. Initiating a dialogue also demonstrates to the requesting authority that the company is taking its request seriously and is endeavoring to respond appropriately.

— ***Try to determine what is motivating the request.*** Keeping an open dialogue will not only build trust, but may help in determining which of the requests is most important to the relevant agency. In turn, this can help the company propose ways to narrow the focus of the request in a way that alleviates the burden on the company while getting the government what it is most interested in as quickly as possible.

— ***Propose an investigative strategy.*** Propose search terms and custodians for a document review, and consider offering to conduct a limited internal investigation short of a full-blown review to determine whether there may be additional ways to reduce the scope of the initial request. In seeking to narrow a request, it is critical to ensure the government understands that the company is not simply seeking to avoid unnecessary burden, but also to increase the efficiency of the investigation.

— ***Propose a schedule, including rolling productions.*** If the information requested will take considerable time to review and prepare for production, for example, due to the volume requested or data restrictions in other jurisdictions, consider proposing a schedule for providing partial responses on a regular basis through rolling productions. To the extent possible, such productions should be organized in a logical manner (e.g., by date, topic, or custodian), and with input from the requesting authority.

— ***Schedule regular check-in calls.*** After an initial conversation is had, regular "check-in" calls to discuss productions and the progress of the investigation serve to keep lines of communication open, apprising the requesting authority of progress while simultaneously helping the company proactively gauge whether the requesting authority is satisfied with the company's response to date. This helps the company steer its investigation in real time, rather than receiving after-the-fact notification that productions have been off-base or insufficient.

— ***Always do what you say you will.*** As discussed, credibility and rapport are critical to maintaining a smooth investigative process. As such, it is almost always better to be upfront about challenges and realistic about timeframes. While a company must avoid creating the impression that it is stonewalling an agency, overpromising and then needing to seek extensions or changes to the investigative plan is almost always worse than proposing reasonable deadlines, explaining why they are necessary, and sticking to them. Indeed, such frankness will often pay dividends both when it is necessary to revise a schedule and when negotiating a resolution at the end of the road.

Requests for Voluntary Disclosure

Government authorities also often request voluntary production of information. The reasons the government may issue voluntary requests can vary, but may include that the relevant regulatory or law enforcement authority (i) has not reached the stage of an investigation where it has compulsory power to issue subpoenas; (ii) views the company as merely a fact witness (as opposed to the target or subject of an investigation) and determined that seeking voluntary disclosures reflects a less aggressive posture; or (iii) determined that the company is, in any event, likely to comply fully with a voluntary request given the desire to remain on good terms with regulators and other authorities. From the company's perspective, it is frequently beneficial to receive a voluntary request rather than a compulsory request. Such voluntary requests not only do not have the force of law, but also may not give rise to the same disclosure issues as compulsory requests.[72] Voluntary requests may be made in the form of a letter or orally. A number of factors inform whether and to what extent a company should comply with a voluntary request for information,

[72] For further discussion of disclosure obligations, *see* Chapter IX: Collateral Considerations.

including the likely benefits of voluntary cooperation, the drawbacks of providing the law enforcement or regulatory agency with information it may not otherwise be able to obtain, and the legal barriers to complying fully with a voluntary request.[73]

In general, a voluntary request may provide more leeway for the recipient to frame the inquiry, as authorities may be more amenable to negotiating the scope of a request in the case of voluntary disclosure. Additional reasons to respond to a voluntary request include the ability to proactively build a positive rapport with the investigating authority (especially one with which the company is likely to come into contact in the future in the event that the agency concludes there has been wrongdoing), and to receive credit for cooperation, which may potentially reduce penalties down the line. In addition, the recipient of a voluntary request should not forget that the requesting authority likely has the power to issue a compulsory request if it deems an entity's voluntary response to be inadequate. Thus, a voluntary response may be viewed as an opportunity to avoid being subjected to a formal investigation. When presented with a voluntary request, therefore, the key objective is to strike a balance between providing a satisfactory response while maintaining the appropriate limitations on disclosure.

In responding to a request for voluntary disclosure, a company should similarly consider the points discussed above in the context of compulsory requests. However, where disclosure will be made voluntarily, the company may have greater latitude in framing its response, including whether to withhold information. This stands in contrast to a compulsory request, where the company risks being penalized if it withholds information absent a legal restriction on its ability to produce the information requested. Thus, in the context of a voluntary request, further consideration may be given to how best to respond while reducing the burden on the company, and making suggestions to the requesting agency to achieve this balance.

[73] Considerations relating to voluntary disclosures are discussed in further detail in the context of cooperation in Chapter VII: Cooperation.

PRACTICE TIP:
CONSIDERATIONS IN RESPONDING TO VOLUNTARY REQUESTS

Potential benefits:

— Ability to build a positive record and gain credibility.

— Potential to receive cooperation credit, which could lead to leniency.

— Increased latitude to frame the inquiry and potentially avoid a subsequent compulsory request.

Potential drawbacks:

— Potential to provide information to which a requesting authority may not otherwise have access.

— Lack of control over how authorities will utilize the information provided.

— Confidentiality concerns and disclosure restrictions.

— A company may be restricted from producing certain documents or information absent a compulsory request.

Conclusion

In sum, a company should give early consideration to the best method of providing the requested information as effectively and expeditiously as possible, regardless of whether the request is compulsory or voluntary. If the company has an obligation to respond or the investigating authority has jurisdiction, an overarching goal may be to provide a satisfactory response while advocating for the most favorable outcome to the company. Thus, giving due consideration at the outset to the various issues that may come into play will go a long way in strategizing how to frame an appropriate response and potentially negotiating the scope of the request. This will not only facilitate the progress of the investigation and garner credibility with the requesting authority, but will also help increase the likelihood of obtaining a favorable outcome.