Surviving a Regulatory Inquiry

Regulators are using increasingly aggressive tactics in seeking information during an inquiry or investigation. However, there are a number of steps that may be taken to reduce costs, minimize the impact on resources, and protect sensitive and confidential information that can be the difference between a merely unpleasant experience and a catastrophic one.

By Gregory Mocek & Joseph Moreno

IN RECENT YEARS, United States regulators, such as the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC), have used increasingly aggressive tactics in seeking information during an inquiry or investigation. Similarly to banks, unregulated commercial trading houses are now facing regulatory scrutiny for their commodity trading.

Under such circumstances, information demands can be extremely broad, time limits are often unrealistic, and the penalties for non-compliance are severe. Surviving such an ordeal can be tremendously costly in terms of time, money, and reputational damage. However, there are a number of steps that may be taken to reduce costs, minimize the impact on resources, and protect sensitive and confidential information that can be the difference between a merely unpleasant experience and a catastrophic one.

Negotiate the Terms of the Request

It has become routine for regulators to issue exceedingly broad information requests and require compliance within an impossibly short deadline. This is because frequently at the initial stage, an inquiry or investigation is fluid and regulators are still formulating their thoughts about potential violations. In order to ensure they capture all possible relevant information, their requests often go far beyond the true scope of the matter. In many cases, information requests are simply regurgitated versions of previous document requests used in other, possibly unrelated, matters. They are often made seemingly without any consideration for the time and resources needed to fully comply.

Rather than adopting an aggressive posture, it can be much more effective to attempt to negotiate the timing and scope of the request

The first reaction to what may appear to be a "fishing expedition" is to come out fighting. Regulatory subpoenas are not self-executing, meaning that although a subpoena is written in the form of a demand, the regulator must go to court to enforce its subpoenas if the recipient chooses not to comply. While it is possible to contest a regulator's subpoena, such challenges are rarely successful. The United States Supreme Court has consistently upheld an agency's authority to enforce subpoena requests so long as the information "is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant."

Rather than adopting an aggressive posture, it can be much more effective to attempt to negotiate the timing and scope of the request. At the initial phase of an investigation, regulators will be unwilling to divulge their case theory which will make negotiations that much more difficult. However, spending some time contemplating the government's case can help bolster an argument as to why it would be in the regulator's interest to make a more targeted information request. You may not convince them to narrow their investigation, but perhaps they will see the value in focusing it. Try to negotiate irrelevant subsidiaries and affiliates out of the demand, narrow the date range, and limit the number of document custodians.

Another effective strategy is to prepare a set of search terms and request that the regulator approve and add to them as they see fit. This way, there is less room later for accusations that search efforts were inadequate.

Most importantly, negotiate a realistic production timetable. Be prepared to make regular updates and to discuss the logistical and technical issues you expect to face in collecting, reviewing and producing the information. Request permission to make partial productions on a rolling basis, and alert the regulator in advance of any anticipated delays. While technical glitches or minor holdups may be explained, nothing will undercut a regulator's confidence in one's cooperation more than repeatedly missing production deadlines.

Identify & Preserve Responsive Information

Immediately upon receipt of an informal demand or subpoena, take steps to identify and preserve responsive information. Issue a written document preservation notice that supersedes your regular retention policy, and be sure to suspend routine deletion of paper or electronic files. Employees should be instructed to preserve all potentially responsive documents, and a custodian of record should be appointed who will be responsible for tracking compliance with the regulator's request. If responsive information is later found to have been intentionally altered or destroyed, a recipient may find itself facing criminal charges of making a false statement or impeding or obstructing a government investigation.

Protect Privileged & Confidential Data

Before producing any information, first conduct a thorough review for information that may be legally privileged. Under United States law, this includes documents protected by the attorney-client privilege, as well as those subject to the attorney work product doctrine. Record the details of all documents withheld from production in a privilege log, and be prepared to present the log and defend any assertions of privilege if challenged. Mark all produced documents with a caption requesting confidential treatment to prevent them from being released under the Freedom of Information Act.

Invariably, privileged documents can fall through the cracks and into regulators' hands. Under the Federal Rules of Evidence and local Bar Rules, a recipient still possesses recourse in the event that privileged information is inadvertently produced.

For example, Federal Rule of Civil Procedure 26(b)(5)(B) states that "if information produced in discovery is subject to a claim of privilege or of protection as trial preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved." While this rule does not govern administrative investigations, it provides certain guiding principles with respect to produced documents and communications.

Employees should be instructed to preserve all potentially responsive documents, and a custodian of record should be appointed

Furthermore, regulators in the District of Columbia may also have an ethical obligation to return privileged documents. Under District of Columbia Bar Rules 1.15(a) and 8.4(c), an attorney has an obligation not to read or use documents, and to return documents to the sending attorney, where it is clear to the receiving attorney that the communication is privileged and was inadvertently disclosed.

In certain cases, regulators may also permit the withholding or redaction of documents that may not otherwise be legally privileged. These may include documents relating to employee compensation, succession plans, merger and acquisition activity, classified government contracts, national security matters, and other confidential and sensitive information. If a subpoena recipient has concerns about the release of such information, make this a point of negotiation with the regulator.

Review Communications

Communications between corporate employers and in-house legal and compliance personnel may be privileged, depending on the nature of the communication and where it is made. In the United States, confidential communications involving in-house counsel are potentially eligible for privilege protection, provided the communication was made for the purpose of obtaining legal advice or services. The privilege may also extend to communications involving compliance personnel who may be attorneys, or may act at the direction of an attorney. This will generally depend on whether the communication was offered in a professional legal capacity.

Regulators have long asserted their reach beyond the borders of the United States ...

This analysis may be difficult when dealing with communications made by in-house attorneys with multiple responsibilities, some of which do not involve providing legal advice. In these cases an attorney's title or position is not always dispositive. While an argument may be made that an attorney who is part of a company's legal department is giving legal advice when communicating with the company's employees, the converse position may be adopted that communications by personnel who are attorneys but who work in management or operations are presumed not to constitute legal advice. The question should be asked – "which hat, legal or otherwise, was the employee wearing at the time they made the communication, and was it made for the express purpose of giving legal advice?"

In most European Union (EU) countries, whether protection applies depends on the status of the lawyer making the communication. The privilege is limited to communications prepared by an "independent" lawyer who is a member of an EU Bar Association [which excludes in-house and non-EU qualified lawyers].

It is somewhat broader in the United Kingdom, whose legal advice privilege applies to communications between a company and members of legal professional bodies such as solicitors and barristers (including qualified foreign lawyers), and includes legally-qualified in-house lawyers acting in a legal capacity. It does not extend to compliance personnel, even when providing legal advice, unless that person also has formal legal qualifications.

Responding to Cross-Border Data Requests

Regulators have long asserted their reach beyond the borders of the United States to activity that affects American markets and consumers. Courts historically permitted the application of United States securities and commodities laws overseas despite the lack of clear language providing for extraterritorial jurisdiction. While this practice was recently scaled back by the US Supreme Court in the landmark case, *Morrison v. National Australia Bank Ltd.,* Congress subsequently provided for extraterritorial application of certain aspects of the securities laws in the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Foreign individuals and companies facing a regulatory demand from a United States regulator must be wary of a number of issues. In the EU, the Data Protection Directive regulates the export of "personal data" to jurisdictions outside the European Economic Area (EEA). This includes any information that "relates to" an identified or identifiable individual, such as home address, personal or work email address, telephone numbers, salary, medical history, tax records and bank statements. In the United Kingdom, the Directive is implemented by the Data Protection Act 1998 (DPA) and is enforced by the Information Commissioner's Office (ICO). Violations may lead to criminal liability and civil penalties of up to £500,000.

Despite these laws, US courts could enforce subpoenas extraterritorially. In such situations, recipients have several options to avoid a potential civil or criminal contempt order.

- **Consent.** You may transfer personal data outside the EEA if you have the affected individual's unambiguous consent to do so. Some nations permit consent to be obtained through the terms of a routine employment contract, while others require it to be collected on a case-by-case basis. However, relying on one individual's consent may be problematic since the information being transferred may contain personal data relating to other individuals who have not consented to its export.
- **Legal Proceedings.** The Directive provides that personal data may be exported if necessary or legally required on public interest grounds. Whether compliance with a foreign (non-EEA) subpoena or court order will qualify depends on the data privacy laws of the particular nation. In the United Kingdom, the DPA permits the export of personal data for the purpose of complying with legal proceedings, and the ICO has provided guidance that this includes foreign legal proceedings. In other countries, subpoena recipients should verify that the need to comply with a United States subpoena qualifies for this exemption. Use of this exemption also requires data export to be limited to only the information that is strictly necessary to comply with the terms of the subpoena or court order.
- **Seek an Exemption.** Most courts will be reluctant to enforce a subpoena if the recipient can show a good faith attempt was made to obtain an exemption from the applicable data privacy law.

Rather than utilising subpoenas, over the last ten years, regulators have sought to obtain foreign information using other alternatives. In 2002, the International Organization of Securities Commissions created a Multilateral Memorandum of Understanding (MMOU) among international regulators. Both the CFTC and the SEC are signatories, as is the UK's Financial Services Authority (FSA) and numerous other European financial organizations. The MMOU allows regulators to exchange information in investigating cross-border violations, and they use it to enforce compliance with securities and derivatives laws and regulations. In addition, both the CFTC and the SEC are signatories to a separate multilateral agreement with the FSA in which all parties pledge to share information needed as part of an investigation, enforcement proceeding, or criminal prosecution.

Conclusion

Aside from the cost, time and anxiety of defending against a regulatory inquiry or investigation, there are a number of legal pitfalls that can arise if not properly navigated. Good faith efforts to cooperate can be undercut by missed deadlines, improper privilege calls, and a variety of technical production issues. Data protection violations may result in significant fines. To guard against these and other unforeseen events, be sure to retain experienced defense counsel who is familiar with the regulator, keep the lines of communication open, and above all, operate in good faith. •

... be sure to retain experienced defense counsel who is familiar with the regulator, keep the lines of communication open, and above all, operate in good faith

Gregory Mocek is a partner at Cadwalader, Wickersham & Taft LLP and the head of the firm's Energy and Commodities Enforcement Defense team. He was formerly the Director of Enforcement for the US Commodity Futures Trading Commission.

Joseph Moreno, a special counsel in the firm's Business Fraud and Complex Litigation Group, formerly served as a federal prosecutor with the US Department of Justice in the National Security Division.

www.cadwalader.com