

March 2021

Follow @Paul\_Hastings



## *U.S. Criminal Antitrust Enforcement: How to Respond When the FBI Comes Knocking*

By [Michael Spafford](#) & [Noah Pinegar](#)

Recent developments presage a return to a more vigorous U.S. criminal antitrust enforcement. For just the second time in history, in January 2020, the U.S. [extradited a defendant](#) from Europe to face U.S. charges of price fixing. The third time followed two months later.<sup>1</sup> DOJ also indicted several executives in 2020 for price fixing in broiler chickens, generic drugs, online government auctions, insulation installing, commercial flooring, ready-mix concrete, radiation oncology, and aluminum structure projects sold to the North Carolina Department of Transportation. In the last three months, for the first time in the 130-year history of the Sherman Act, an agreement not to compete for the hiring of employees was treated as a criminal violation.<sup>2</sup> That the Justice Department [warned of its novel approach](#) in 2018 does not make it any less dramatic. Combined with a [new focus](#) by Congress and the Biden Administration on antitrust laws and remedies, it appears that criminal enforcement is likely to return to pre-2016 levels or higher.

In anticipation, companies should update their antitrust compliance program and procedures to meet and exceed the requirements of the Antitrust Division's new 2019 compliance policy, which permits prosecutors to credit the effectiveness of a compliance program at the charging stage, and not just at sentencing. The policy provides valuable guidance as to what the Antitrust Division considers important when evaluating antitrust programs for the purposes of determining credit.<sup>3</sup>

Companies should also prepare for how to respond when there is a knock at the door and it is the FBI. The execution of a search warrant on a company can have a significant impact on a company's officers, employees, and customers, disrupt normal business operations, and affect a company's ability to defend itself against potential criminal charges. When a search warrant is executed, a company frequently receives no more warning than a "knock on the door," followed by an intrusive and disruptive raid of offices and facilities for documents, electronic materials, and physical evidence. It is therefore imperative to understand and prepare for what to do when the FBI appears—unannounced—with a search warrant.

Defining roles ahead of time and developing procedures in advance for how to respond can avoid problems or misunderstandings if and when the FBI comes knocking. FBI visits can come in many forms—from one or two agents appearing at your door to a team of agents (including U.S. Postal Service or other agency personnel) performing an expanded visit or raid at one or more locations. These procedures apply regardless of the size or composition of the FBI team.

## **AHEAD OF TIME**

### **I. Designate and train a response team.**

Responsibilities should be clearly defined. Four roles, performed by separate employees, where practical, follow (depending on your organization and number of locations, it may be appropriate to have multiple employees fill each role for different units or locations or combine roles where appropriate):

One person will LEAD the company's response during and after the search. This person will know the company's plan for responding ahead of time, and will take charge of the company's response during and after the search. This does not have to be an attorney, although there may be advantages to having an attorney, if possible, in this role. The LEAD should promptly notify the Office of the General Counsel of the FBI visit.

Another person will MANAGE COLLECTION of electronically stored information and IT equipment and personnel. That person should be familiar with the structure of the company's data and experienced with copying data. They should also know how and where legal department materials (potentially privileged) are maintained so that they can be clearly identified. FBI agents may work around those materials, or they should at least be kept separate until outside counsel and the government agree on how to resolve the issue.

A key employee should MONITOR the searching agents and take notes about areas searched, property seized, and anyone that speaks with the agents.

Another person will be responsible for COMMUNICATING with employees about their rights and responsibilities.

### **II. Establish procedures and guidelines for what to do when the FBI shows up.**

These should supplement your antitrust compliance program. Certain COMMUNICATING employees can be prepared ahead of time to advise employees. Guidance to employees should include:

- All employees should be polite and avoid interfering with or disrupting the agents' activities. Employees should be cooperative with the agents, but also know their rights.
- Employees may, but do not have to, communicate with the agents and do not have to discuss the substance of the investigation during the search. Employees can limit their communications to assisting in locating materials to expedite the execution of the search warrant.
- Advise your employees that the company will provide them with counsel to represent them at no cost to the employees if requested.
- Employees should be instructed not to remove, discard, or conceal anything that might be responsive to the search warrant or related to the investigation.

The role of MANAGING COLLECTION personnel requires familiarity with document retention procedures ahead of time so they are prepared, for the moment when the search warrant is executed.

## **THE FBI KNOCKS AT THE DOOR**

### **III. Specific guidance for during the search.**

- Be courteous and cooperative.

- You have a right (and a fiduciary duty) to maintain your operations and negotiate ways to limit the disruption to the company.
- The LEAD may ask if the search can be conducted at the conclusion of the workday, with the assurance that all records will be maintained.
- The COMMUNICATING role should contact the Office of the General Counsel and/or outside counsel immediately.
- The COMMUNICATING role should advise employees of the company's guidance during the search.
- The LEAD identifies themselves to the agent in charge. The LEAD obtains the name and phone number of the government attorney in charge of the investigation from the warrant or from the agent in charge.
- The LEAD requests and reviews a copy of the search warrant and all supporting materials. If not provided a copy of the search warrant, do not consent to a search without first contacting criminal defense counsel.
  - Only the places and items identified in the search warrant may be searched and seized.
  - Request an inventory of all items seized.
  - Ask the agents to complete the search first and then discuss the substance of the investigation with employees at a later date.
  - The MONITOR must also review or know the limits of the search warrant so they can identify, both in their notes about the search and courteously to the agents, if the search exceeds the scope of the search warrant.
- The employee MANAGING COLLECTION may ask that the agents image hard drives rather than seize computers.
- If electronic media or hardware is seized, the employee MANAGING COLLECTION should request a backup disk, and may ask to assist in copying the data or disconnecting the hardware to avoid damage.
  - Ask to maintain originals and provide copies (or, in limited circumstances, provide originals and maintain copies).
- You have a right (and a duty) to protect your company's privilege.
  - For documents where the privilege is clearly implicated, such as an attorney's files, the MONITOR should suggest that the items be produced pursuant to a grand jury subpoena to allow for a privilege review.
  - If the agents insist on removing potentially privileged items, the MONITOR should request that they be maintained separately and not be reviewed until your attorney and the government attorney in charge of the investigation agree on how to resolve the issue. Request permission to copy or to prepare a detailed inventory of these documents.

- If privileged materials cannot be segregated, such as email housed on a server, the MONITOR should inform the agents of this and request that none of the materials so stored be reviewed until your attorney agrees to an appropriate privilege review process.

## AFTER THE SEARCH IS OVER

### IV. Actions after the search.

Working with in-house and outside counsel, the LEAD and MONITOR should conduct an internal investigation, retracing the FBI steps to figure out what the FBI was looking for and what materials were copied or taken pursuant to the search warrant.

Outside counsel should follow up with the lead government attorney about the documents, including any privileged materials, and the parameters of the investigation.

The COMMUNICATING role should send a formal document retention notice, along with regularly scheduled reminder notices, to all employees potentially in possession of materials related to the subject matter of the investigation.

The MANAGING COLLECTION role should preserve electronic storage, pausing any auto-delete functions to preserve data for forensic collection working with outside counsel (including any back-up materials).

Although infrequent and unwanted, search warrants come without warning and can be highly disruptive. Planning is needed to enable a company to respond effectively when the FBI comes knocking. Otherwise, mistakes or worse may occur. As with any such matters, consulting with outside counsel helps ensure the implementation of appropriate safeguards and policies to manage antitrust compliance risks, including the risk of a “knock at the door.”

◇ ◇ ◇

*If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:*

#### Century City

Bo Pearl  
1.310.620.5730  
[jamespearl@paulhastings.com](mailto:jamespearl@paulhastings.com)

#### Washington, D.C.

Michael L. Spafford  
1.202.551.1988  
[michaelspafford@paulhastings.com](mailto:michaelspafford@paulhastings.com)

Michael S. Wise  
1.202.551.1777  
[michaelwise@paulhastings.com](mailto:michaelwise@paulhastings.com)

#### San Francisco

Thomas P. Brown  
1.415.856.7248  
[tombrown@paulhastings.com](mailto:tombrown@paulhastings.com)

Gary Zanfagna  
1.202.551.1940  
[garyzanfagna@paulhastings.com](mailto:garyzanfagna@paulhastings.com)

Noah Pinegar  
1.292.551.1960  
[noahpinegar@paulhastings.com](mailto:noahpinegar@paulhastings.com)

---

<sup>1</sup> The U.S. has provided cooperation to allies' criminal authorities as well. The U.S. recently agreed to extradite two citizens to Japan in connection with a Japanese criminal investigation of the Ghosn affair.

#### Paul Hastings LLP

PH Perspectives is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2021 Paul Hastings LLP.

- 
- <sup>2</sup> The former owner of a health care staffing company was indicted for wage-fixing in December. See <https://www.justice.gov/opa/pr/former-owner-health-care-staffing-company-indicted-wage-fixing>. Then, in January, a separate indictment charged that an outpatient care company conspired with another company to not recruit senior-level employees employed by the other. See <https://www.justice.gov/opa/pr/health-care-company-indicted-labor-market-collusion>.
- <sup>3</sup> See U.S. Dep't of Justice Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (July 2019), <https://www.justice.gov/atr/page/file/1182001/download>.