LEGAL & REGULATORY

RESPONDING TO U.S. SEARCH AND SEIZURE WARRANTS AND EU DAWN RAIDS

REPRINTED FROM:
JULY 2010 ISSUE

FW MAGAZINE
FINANCIER WORLDWIDE corporatefinanceintelligence

LEGAL & REGULATORY

LITIGATION

Responding to US search and seizure warrants and EU dawn raids

BY DAN GOLDFINE

Twenty years ago, searches/seizures and dawn raids to investigate business crimes, fraud and wrongdoing were largely unheard of. Investigators at that time asked businesses for the records and voluntary cooperation; on occasion, grand juries and other investigatory bodies served subpoenas and compelled oral testimony. A new era of EU cartel enforcement and, in the US, the collection of billions of dollars in criminal fines and forfeitures and controversies surrounding Enron, Madoff, Goldman Sachs, private bribery cases, and devastating oil spills over the last 20 years have changed that. Wrongful business conduct has been thoroughly 'criminalised', and investigators now use tactics previously reserved for investigating organised crime and drug dealers, including searches/seizures and raids. The use of these investigatory tactics has become more frequent and visible. This means that company executives and in-house counsel should take steps to plan for their possibility.

Unfortunately, few in-house counsel or company executives have been trained on how to handle searches/seizures or dawn raids or have personally experienced such tactics. These tactics are extremely intimidating to executives, employees, and in-house counsel – as they are intended to be. Investigators use them to gather physical evidence, documents and electronic documents, data and metadata, but also to create an environment of fear, distrust, intimidation and compulsion – hoping to create circumstances and an environment whereby executives and employees make statements that they would not otherwise make. More often than not, these statements are made outside the presence of company counsel or a witness to ensure accuracy and completeness as well as simply knowing what has been said to investigators, giving investigators tactical advantages relative to the company's and executives' defences.

Know what to expect

Some generalisations can be made. Given that other mechanisms more effectively and efficiently collect documents and data than searches/seizures and dawn raids, the fact that they provide an opportunity for controlled interviews, outside the presence of counsel, of unprepared executives and employees in an intimidating setting often drives the raids. Likewise, investigators may be employing the raid and seize tactic to interrupt business operations and thereby gain strategic advantage and deprive the target of revenues.

Searches/seizures and raids usually take place in the morning, shortly after the work day begins. It is easier to organise multiple law enforcement agents and agencies at that time. There is greater predictability as to who will be present, and a morning raid allows more time for employee interviews and curing mistakes (e.g., raiding the wrong office). The number of agents ranges from a handful to more than 50. Often, the number of agents correlates to the number of key interviewees located at the site (i.e., two agents for each key interviewee). In the US, the investigators will be ridiculously armed as if they were raiding a heavily-armed fortress.

During raids, investigators typically seize – but not search for days, weeks or months – the company's computers, servers, back-up tapes, and PDAs, severely disrupting business operations – known as the seize-first approach. In the US, the current standard is that US federal and state courts will permit law enforcement to seize and retain these materials for 45 to 90 days. In employing the seize-first approach, investigators often disregard the limits of the warrant (in the US) or the notice authorising the dawn raid (EU) and attorney-client privilege.

Know what to do

Good lawyering in the face of a search/seizure or dawn raid is akin to performing triage during a medical emergency: prevent further harm and prioritise immediate risks. Determine in advance the single executive or in-house counsel who is the sole 'go-between' with investigators. Identify a back-up person. Contact pre-arranged outside counsel immediately. Given attorney-client privilege issues and legal limitations surrounding in-house counsel who is involved in business decisions, the immediate involvement of outside counsel (by telephone or in person) in any discussions involving how to respond or other tactical

decisions is a mandatory requirement.

At the onset of the raid, the 'go-between' and outside counsel should immediately obtain a copy of the warrant (US) or authorising notice (EU). That document will guide the limits and scope of the search and seizure. Do not consent (impliedly or expressly) to any expansion of the scope of the warrant or notice. Absolutely do not sign any document the investigators present without thorough legal review.

The 'go-between' and outside counsel should monitor the search and document any seizures or searches in excess of the permitted scope. (Additional attorneys or their support staff may be necessary.) In the US, contact the prosecutor listed on the warrant immediately if investigators exceed the warrant's scope.

Given that the main purpose is often not the search for and seizure of documents and data but to interview and intimidate unprepared witnesses, send all non-essential employees home or to the movies to reduce that risk. Anticipate that the investigators will attempt to track the company's employees and executives, typically at their homes, and remind the executives and employees that while no obstruction or lying will be tolerated, proper cooperation of company employees is through scheduled interviews for which witnesses have had a fair opportunity to prepare and at which the company and the witness (if necessary) can be represented by an attorney. Also, remind executives and employees that if investigators contact them to contact company counsel.

Instructions on how to handle interviews are more effective if also given in advance. As part of an employee manual and/or training program, companies can give clear written instructions to executives and employees on how to handle encounters with law enforcement and investigators. These instructions should direct executives and employees to have investigators arrange interviews through company counsel and provide employees with clear and updated contact information that they are, for example, free not to submit to an interview at their home or outside the presence of counsel.

The 'go-between' and company counsel should instruct employees who remain behind not to engage in any dialogue or small talk with the investigators. Refer the investigators' questions and inquiries to the 'go-between' or outside counsel. Demand copies of all materials seized, including electronic data and documents. In the US, investigators will not provide copies at the time of the search. In that light, immediately contact the prosecutor listed on the warrant and commence efforts to obtain copies. Rule 41 of the Federal Rules of Criminal Procedure provides a mechanism to obtain copies in the event investigators or prosecutors fail to cooperate.

Searches/seizures and dawn raids are also an opportunity to learn what investigators know about and suspect they will learn from the company. Outside counsel should debrief all executives and employees about the search/seizure or dawn raid immediately. Despite the best efforts of the 'go-between', outside counsel, executives and employees to avoid an interview or discussion with investigators in this setting, such discussions and interviews invariably take place. A contemporaneous record of what executives and employees told investigators and what investigators asked is valuable.

The seize-first approach creates a special problem for the company that does not have access to back-up data and media. In the US, move for an immediate Rule 41(g) Order requiring that any search of electronic data and media be done on-site rather than seizing and holding the company's valuable electronic data and media for months. As a practical matter, any seizure of electronic data and media is especially burdensome, poses a risk of business shutdown, and will capture irrelevant and privileged data and documents that, if such was in hard copy form, investigators would not be able to seize. (Beginning in 2009, US law enforcement takes the position, with no evidentiary support, that overbroad seizures of electronic media, data and documents are necessary (US Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence Manual at Ch. 2.C.3 (2009)). As recently as 2002, US law enforcement took the opposite position (Federal Guidelines of Methods of Obtaining Documentary Materials Held by Third Parties, 28 C.F.R. Part 59 §§ 59.1, 4. US courts are beginning to question the seize-first approach. See, e.g., U.S. v. Comprehensive Drug Testing, 579 F.3d 989, 995 (9th Cir. 2008)).

There are some final considerations. Manage expectations. Help everyone act responsibly, with prudence and without panic. Control disclosure of the investigation. Take steps to ensure that only appropriate disclosure is made by an expressly authorised executive. Finally, since a search/seizure or dawn raid may be the first indication of a government inquiry, it raises issues with respect to whether to conduct an internal investigation, which attorneys can and should conduct that investigation and can and should defend the company in the government's investigation, governance of the internal investigation and defence, preservation of privilege and work product protections, disclosure to auditors, independent director duties, and disclosure to shareholders and potential shareholders. Advance planning to develop procedures and standards with respect to these issues is prudent. ■

Dan Goldfine chairs Snell & Wilmer's Government Investigations group. He can be contacted on +1 (602) 382 6282 or by email: dgoldfine@swlaw.com.

Dan Goldfine is a partner in Snell & Wilmer's Phoenix office and chairs the firm's Government Investigations/White Collar Criminal Defense Group. He defends mid-market and Fortune 500 companies, as well as board committees, directors and management executives, with respect to government and internal investigations. Before joining Snell & Wilmer, Mr. Goldfine was a Trial Attorney with the Antitrust Division of the US Department of Justice where he supervised and participated in overt and undercover government investigations of white collar crime, leading to many convictions of companies and executives.