United States

Latham & Watkins Robert E Sims & Ramin Tohidi

1. INTRODUCTION

In the United States, companies are considered legal persons that can sue or be sued, and can commit or be the victims of crime. Indeed, it is not unusual for a company, especially a large corporation, to simultaneously be the victim or witness in a criminal proceeding in one US jurisdiction while finding itself under investigation for allegedly committing a crime in another US jurisdiction. But whether the company suspects that it is a potential victim or the perpetrator of a crime, it will likely need counsel to conduct a thorough internal investigation to determine the facts and recommend a path forward. Company counsel who diligently investigate credible allegations of serious misconduct will always be better positioned to advise their clients in determining whether and how to: disclose the misconduct to the government; cooperate in any ensuing government investigation; and implement any changes needed to remediate the problem.

US agencies typically are willing to leverage their targets' internal investigative efforts before filing charges or launching a more invasive probe. US prosecutors and judges are more likely to be lenient with companies that voluntarily report suspected wrongdoing and cooperate with the government. And, in cases of victimisation, prosecutors are more likely to charge the perpetrators when a company credibly shows that a crime was committed and offers its investigative support. A company's reluctance to investigate and communicate with the government, on the other hand, often results in added scrutiny and harsher treatment if the government subsequently becomes aware of wrongdoing by the company that it believes should have been reported.

An effective internal investigation accomplishes several goals. It allows a company to determine the facts, gain a clear understanding of the legal landscape in which it operates, assess its potential liability, and identify and preserve the relevant evidence. At the same, a thorough investigation also allows the company to protect confidentiality and avoid any interactions with the government that may prove costly. This chapter addresses each of these important components of an effective internal investigation in the US.

2. MANAGING THE INTERNAL INVESTIGATION

Any general counsel whose company is subject to US laws should have a general understanding of when and to what extent her company may be liable for employee misconduct. She should also be aware of certain best

practices, recommended procedures and common pitfalls in determining how to structure and manage an internal investigation.

Corporate criminal liability

Law enforcement officials in the United States say that the *'[p]rosecution of a corporation is not a substitute for the prosecution of criminally culpable individuals within or without the corporation'* (United States Attorneys' Manual, 9-28.200, available at *http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/title9.htm* (USAM)). It is nevertheless true that numerous investigations and prosecutions each year are resolved against companies alone. And while there are some circumstances, discussed below, where companies cannot be held liable for their employees' misconduct, the prevailing law enforcement view in the US is that companies should generally be *'held responsible for the acts of their employees'* because they *'can only act through'* their employees (id., 9-28.500; see also id., 9-28.200).

Corporate liability under respondeat superior

Corporate liability for employee misconduct derives from the doctrine of respondeat superior. See *United States v Koppers Co.,* 652 F.2d 290, 298 (2d Cir. 1981); *United States v Basic Constr. Co.*, 711 F.2d 570, 572–73 (4th Cir. 1983); *United States v Hilton Hotels Corp.*, 467 F.2d 1000, 1004–07 (9th Cir. 1972); *United States v Beusch*, 596 F.2d 871, 877–88 (9th Cir. 1979). The rule holds that legislatures *'may constitutionally impose criminal liability upon a business entity for acts or omissions of its agents within the scope of their employment'* (*Hilton Hotels Corp.*, 1004; see also id., 1006 (noting that the *'conviction and punishment of the business entity itself is likely to be both appropriate and effective'*); *New York C. & H. R. R. Co. v United States*, 212 US 481, 495–96 (1909) (an alternative *'doctrine that a corporation cannot commit a crime would virtually take away the only means of effectually . . . correcting the abuses aimed at'*)). Thus, statutes that expressly or implicitly contemplate the prosecution of businesses may do so via vicarious liability for employee conduct: see, eg, *Hilton Hotels Corp.*, 1004–07 (finding that Congress intended the Sherman Act to impose corporate criminal liability).

Companies can be held criminally liable for the acts of all employees or agents acting within the scope of their employment, not exclusively senior managers or executives. See *Hilton Hotels Corp.*, 1007 (liability based on the actions of an authorised purchasing agent); *Basic Constr. Co.*, 572–74 (liability resulting from actions of *'two relatively minor officials . . . without the knowledge of high level corporate officers'*); *Koppers Co.,* 298. Corporations, moreover, cannot avoid liability simply because their employees acted contrary to corporate policies or express instructions. See *Hilton Hotels Corp.*, 1007; *Basic Constr. Co.*, 573. The relevant question, instead, is *'whether measures taken to enforce corporate policy . . . adequately insulate the corporation against'* the acts in question (*Beusch*, 878; see also *Hilton Hotels Corp.*, 1007 (corporation *'could not gain exculpation by [management] issuing general instructions without undertaking to enforce those instructions by means commensurate with the obvious risks'*)).

However, for companies to be held vicariously liable, their employees must have intended, at least in relevant part, to benefit them. See *Beusch*, 877*; Hilton Hotels Corp.*, 1006, note 4; *Federal Sav. & Loan Ins. Corp. v Shearson-American Express, Inc.*, 658 F. Supp. 1331, 1338 (D.P.R. 1987). Only acts that an agent does to benefit her employer are properly within the scope of her employment. See *Beusch*, 877; *Hilton Hotels Corp.*, 1006, note 4. However, so long as the intent to benefit is shown, it does not matter that *'no benefit accrue[d], [the] benefit [was] undiscernible, or . . . the result turn[ed] out to be adverse'* (*Standard Oil Co. of Texas v United States*, 307 F.2d 120, 128–29 (5th Cir. 1962); see also *Beusch*, 877–78). The clearest example of an employee's actions falling outside the scope of his employment occurs when the employee intended and caused his employer's injury. See *Standard Oil Co.*, 129; *Union City Barge Line, Inc. v Union Carbide Corp.*, 823 F.2d 129, 138–39 (5th Cir. 1987).

Where proof of knowledge or wilfulness is required

For violations that require proof of knowledge, wilfulness, or some other mental state, the government (expectedly) must prove that particular mental state in order to hold the target company accountable. See, eg, *Standard Oil Co.*, 127. For example, the federal crime of possession of a stolen trade secret requires knowledge that the information possessed was stolen or improperly obtained (18 U.S.C. § 1832). The common rule in such cases is that if an employee – even a subordinate or menial one – acted within the scope of his employment, then by law his employer's mental state is the same as his. See *Standard Oil Co.*, 127; see also *New York C. & H. R. R. Co.*, 481; *United States v George F. Fish, Inc.*, 154 F.2d 798, 801 (2d Cir. 1946).

Where a company's employees were actually ignorant of some actionable fact, liability will still attach if the government proves that those employees were aware of a high probability of the existence of the information and *'deliberately avoided learning the truth'* (*United States v Pacific Hide & Fur Depot, Inc.*, 768 F.2d 1096, 1098–99 (9th Cir. 1985) (defendant may not intentionally avoid gaining culpable knowledge)). Actionable ignorance, or wilful blindness, can also result from *'flagrant organizational indifference'* (*United States v Bank of New England, N.A.*, 821 F.2d 844, 855–56 (1st Cir. 1987)). Companies can be criminally liable when their employees fail to act despite an *'abundance of information'* telling them to do so (id., 857). A corporation also cannot intentionally *'compartmentalize knowledge, subdividing the elements of specific duties and operations into smaller components'*, and thereby defend against prosecutions on the basis that no one of its employees understood the full import of his or her respective knowledge (id., 855–56). Absent evidence of some wilful blindness on the part of the organisation, courts are reluctant to impute to the broader entity the collective knowledge of various employees acting innocently within the scope of their employment.

Effective compliance programme

Companies with robust compliance programmes generally are best prepared to determine when to conduct internal investigations and how to structure and manage them. Effective compliance programmes help prevent and deter wrongdoing, detect compliance problems when they occur and guide the appropriate responses. A programme incentivising employees to report suspected violations (even allowing them to do so anonymously) can serve as an important early warning system for company counsel. For example, a credible report alleging serious wrongdoing by a senior executive could itself compel the company to undertake an internal investigation.

Effective compliance programmes have other important benefits. Prosecutors, in their charging decisions, are likely to credit companies for having effective programmes. See, eg, USAM, 9-28.300 and 9-28.800. The United States Sentencing Commission Guidelines similarly provide for leniency to corporations that implement *'effective compliance and ethics program[s]'* (United States Sentencing Commission Guidelines Manual § 8C2.5(f) (1 November 2013), available at *http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2013/manual-pdf/2013_Guidelines_Manual_Full.pdf* (Sentencing Guidelines)).

Broadly speaking, an effective programme is one that is *'reasonably designed, implemented, and enforced so that [it] is generally effective in preventing and detecting criminal conduct'* (id., § 8B2.1). It should provide for, among other things, organised responsibilities and accountability (including oversight by senior executives or a board committee), standardised reporting procedures, educational programmes, legal review and analysis of potential misconduct, transparency, auditing and procedures for punishment. Compliance programmes should be tailored to fit the relevant business and industry; a company should not expect credit for a 'one size fits all' programme that it does not enforce.

However, even an effective compliance programme is not alone a defence to a claim of respondeat superior (see *Basic Constr. Co.,* 573). Nor does it guarantee that a prosecutor will not pursue claims or charges against the company. The US Department of Justice (DOJ), for example, will not decline to charge a corporation simply because it has a policy – even one that *'specifically prohibit[s] the very conduct in question'* (USAM, 9-28.800).

Yet there is no question that an effective compliance programme helps mitigate the adverse impact of employee misconduct. Companies, especially those operating in high-risk industries or markets, should develop and implement thorough and effective compliance programmes well before finding it necessary to conduct an internal investigation of suspected wrongdoing.

Initial considerations and planning

Once a company determines that an internal investigation is necessary, it must then decide who will conduct the investigation and to whom the results will be reported. The company must also determine whether it is important to keep the contents and results of the investigation confidential

and/or protected by the attorney–client privilege. The answers to these questions vary depending on the circumstances. For example, where a company investigates low-level employees for suspected violations of its code of conduct expected to cause minimal legal exposure, internal audit or corporate security personnel likely can handle the investigation without supervision from counsel. On the other hand, where the general counsel knows that the US government is conducting a criminal inquiry into the conduct of high-ranking company officials, outside counsel almost certainly should conduct a privileged investigation reporting to the company's board of directors.

Many matters will fall in between these two examples, requiring that company counsel consider various factors in structuring the investigation. These factors include: whether, in the particular jurisdiction, the attorney–client privilege applies to communications with in-house counsel; the relative cost of an investigation; and the need for subject matter expertise and external resources. Importantly, these issues should be considered at the outset of an investigation. It is very difficult, for example, to start an investigation that is not protected by the attorney–client privilege and then, based on the interim results, convert the investigation to one that is privileged.

In choosing outside counsel to conduct an investigation, it may be appropriate for a company to retain its regular corporate or litigation counsel, assuming that such counsel has the requisite experience and expertise. Attorneys who are already familiar with the company and understand its business will often be able to conduct an internal investigation more efficiently than new counsel. Where it is necessary for the company to demonstrate the independence of an investigation – for example, where the conduct of very senior company officials is at issue – it may be necessary to retain counsel with no previous relationship with company management.

Privilege and work product

A business entity is entitled to the attorney–client privilege and attorney work product protection (*Upjohn Co. v United States*, 449 US 383, 388–97 (1981)). These safeguards extend to internal investigations conducted at the direction of counsel (id.; see also *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 756 (D.C. Cir. 2014) (citing *Upjohn*)).

In order for a company to protect communications made between its employees and its lawyers, counsel should always advise its employees that they are participating in a privileged investigation and should keep confidential everything discussed with counsel. So long as the communications are kept private, relate to the employees' scope of employment, and allow counsel to give legal advice to the company, the communications should remained privileged unless and until the company chooses to waive that privilege. See *Upjohn*, 394; see also id., 388–97. The notable exception here is any communication *'made in furtherance of a crime*

or fraud' (USAM, 9-28.720 (citing *United States v Zolin*, 491 US 554, 563 (1989); *United States v BDO Seidman, LLP*, 492 F.3d 806, 818 (7th Cir. 2007))).

Attorney work product prepared during the course of an internal investigation might be discoverable when it contains facts that are otherwise unavailable but are needed as evidence. See *Upjohn*, 399 (citing *Hickman v Taylor*, 329 US 495, 511 (1947)). However, work product that contains 'opinions' – ie the mental impressions, conclusions, opinion or legal theories of an attorney – generally cannot be discovered. See *Upjohn*, 399–400 (citing Fed. R. Civ. Proc. § 26). Work product materials that contain lawyers' written thoughts therefore will almost certainly remain protected from disclosure.

All documents transmitted and generated during a privileged internal investigation, including email communications, should be clearly marked as privileged communications or work product, as applicable. If non-lawyers are participating in the investigation at the direction of counsel (eg private investigators or internal audit personnel), they should be reminded to mark their own communications related to the investigation as privileged – even those communications to which counsel is not a party.

Waiver

According to the DOJ, the *'attorney–client privilege and the attorney work product protection serve an extremely important function in the American legal system'* (USAM, 9-28.710), and therefore *'[e]ligibility for cooperation credit [for charging and disposition decisions] is not predicated upon the waiver'* of either one (id., 9-28.720). However, when companies *'are victimized by their employees or others'*, prosecutors expect them to freely waive their protections and *'seek prosecution of the offenders'* by disclosing *'the details of [their] investigation'* (id., 9-28.710).

Companies should not undertake lightly any decision to waive privilege or work product protections. In almost all federal jurisdictions, privilege waivers for materials disclosed to the government will extend to any other subsequent litigant. See, eg, *Pac. Pictures Corp. v United States Dist. Court*, 679 F.3d 1121, 1127 (9th Cir. 2012); *In re Qwest Commc'ns Int'l, Inc. Sec. Litig.*, 450 F.3d 1179, 1201 (10th Cir. 2006); *Burden-Meeks v Welch*, 319 F.3d 897, 899 (7th Cir. 2003); *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 295 (6th Cir. 2002); *United States v Mass. Inst, of Tech.*, 129 F.3d 681, 686 (1st Cir. 1997); *Genentech, Inc. v United States Int'l Trade Comm'n*, 122 F.3d 1409, 1416–18 (Fed. Cir. 1997); *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 236 (2d Cir. 1993); *Westinghouse Elec. Corp. v Republic of Philippines*, 951 F.2d 1414, 1425 (3d Cir. 1991); *In re Martin Marietta Corp.*, 856 F.2d 619, 623–24 (4th Cir. 1988); *Permian Corp. v United States*, 665 F.2d 1214, 1221 (D.C. Cir. 1981); cf. *Diversified Industries, Inc. v Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (en banc) (concluding that client did not waive attorney client privilege over material voluntarily surrendered to the SEC pursuant to an agency subpoena). The rationale against the 'selective waiver' rule is that it would not *'serve the purpose of encouraging full disclosure to one's attorney'* but, rather, only one's voluntary disclosure to the government,

which is not the intended purpose of the privilege (*Pac. Pictures Corp.*, 1127 (citing *Westinghouse Elec. Corp.*, 1425)).

Waiver can also extend to any undisclosed documents or portions of documents relating to the subject matter of any documents disclosed. See, eg, *In re Sealed Case,* 877 F.2d 976, 980–81 (D.C. Cir. 1989); *Genentech, Inc.*, 1416–17; *In re Grand Jury Proceedings*, 78 F.3d 251, 255 (6th Cir. 1996)*; In re Continental Illinois Sec. Litigation*, 732 F.2d 1302, 1314, note 18 (7th Cir. 1984). This subject matter waiver rule prevents *'the inequitable result that the waiving party could waive its privilege for favorable advice while asserting its privilege on unfavorable advice'* and thereby improperly use the privilege *'as both a sword and a shield'* (*In re EchoStar Communs. Corp.*, 448 F.3d 1294, 1301 (Fed. Cir. 2006) (citing *XYZ Corp. v United States*, 348 F.3d 16, 24 (1st Cir. 2003))). Any given *'subject matter can be defined narrowly or broadly'*, and thus trial courts must determine the scope of a waiver on a case by case basis. See *In re Grand Jury Proceedings*, 255-56 (citing *In re Sealed Case*, 981) (finding disclosure of advice on specific items of marketing plan did not constitute waiver of privilege for the entire plan).

Document collection and review

Most investigations should begin in substance with a thorough review of the relevant documents. While counsel may benefit from prior employee interviews to better understand the issues and potential sources of information, substantive interviews of company personnel should generally follow a detailed understanding of the written record.

In most investigations in the United States, there are no legal limitations on searching company files and property for relevant information. Counsel should, however, review applicable state law, as some states prohibit, or provide civil claims for, invasive searches in the workplace. Even so, most company policies and employment agreements in the US give wide latitude in searching work-related materials.

Routine document destruction should already have been suspended (as discussed below in section 4, 'The duty to preserve evidence'). In many cases, counsel will retain an e-discovery consultant to collect electronic data and host it on a searchable review platform. Counsel should also arrange for someone at the company (or a discovery consultant) to gather all responsive hard copy documents. All privileged and/or confidential materials should be identified, segmented and indexed as part of the review process.

Document review and analysis is often the most time-consuming portion of an investigation. Once the legal team is confident that all relevant documents and data have been collected, reviewed and analysed, it can begin to organise that data for use in the investigation, including during employee interviews.

Conducting employee interviews

Personnel interviews are usually critical to internal investigations. The purpose of these interviews is to fully explore employees' knowledge about the subject matter of the investigation. This will usually include

having the employee explain or provide additional information about relevant documents and determining whether the employee is aware of any previously undisclosed allegations, information or materials.

Counsel should evaluate who will participate in each interview. In most cases, two people (each usually company counsel) should participate so that one can act as the primary note-taker and serve as a witness if there is a subsequent dispute about the interview in any criminal or civil proceeding. In some circumstances, it may be appropriate for company counsel to consider whether an employee needs separate counsel to represent the employee individually. Though this is not routinely done, retaining separate counsel may be advisable, for example, when company counsel anticipates or is aware of a government investigation, there is evidence that the employee to be interviewed may be culpable and the company believes that individual counsel is needed to protect the employee's interests.

Each interview should begin with so-called *Upjohn* warnings. Counsel should admonish the interviewee that he represents the company, not the employee, and that he is not giving the employee any legal advice. Counsel should also advise that the interview is privileged as part of an ongoing confidential internal investigation and that the interviewee should keep private anything discussed during the interview, but that the company may choose to waive privilege and disclose the findings of the investigation to outside parties. It is important that the interview notes and any related memoranda reflect the fact that counsel provided these standard *Upjohn* warnings.

Reporting findings to the client and the government

After an internal investigation is complete, counsel should prepare a summation of its findings and recommendations. This final report to the company (or its board of directors or board committee) need not be written, however. Counsel may instead prepare internal talking points and deliver its analysis to its client via an oral presentation.

Although a written report has its obvious uses, if the company's intent is ultimately to coordinate with law enforcement, the company should expect that the government will ask for it. Auditors, opposing parties in litigation, regulators and other third parties may also seek to obtain copies of written reports. In complying with those requests, the company could risk waiving privilege over the report and any other otherwise privileged communications concerning the same subject matter (see 'Privilege and work product' above). Therefore, in most circumstances, the safer course is simply to provide a verbal report to the company that includes a set of the relevant documents found during the investigation.

If the matter under investigation involves criminal wrongdoing, the company should evaluate the benefits of voluntary disclosure in light of the risks. Voluntary disclosure may induce prosecutorial leniency. See, eg, USAM, 9-28.300 (*'In conducting an investigation, determining whether to bring charges, and negotiating plea or other agreements, prosecutors should consider . . . the corporation's timely and voluntary disclosure of wrongdoing and its willingness*

to cooperate in the investigation of its agents'). Prosecutors are more often willing to enter into non-prosecution or deferred prosecution agreements with companies that make voluntary reports. Such agreements allow companies to avoid felony charges. Voluntary disclosures may also result in decreased fines under the Federal Sentencing Guidelines. See Sentencing Guidelines § 8C2.5(g). Also, where a company is the victim of employee misconduct, disclosure may assist the prosecution, and thus increase the likelihood of restitution or the deterrence of future employee wrongdoing.

The risks of making a voluntary disclosure are often obvious. The company may bring a matter to the government's attention that it might otherwise have missed and subsequently use against the company. The voluntary disclosure may be characterised later as a waiver of the attorney–client privilege or work product protection. An ongoing criminal investigation or prosecution can also sometimes interfere with any related civil litigation the company may pursue.

3. DISCLOSURE FROM THIRD PARTIES

In the United States, there are few means of requiring third parties to disclose documents outside of a pending lawsuit. A particular vendor contract, for example, may provide a company with the right to audit the vendor's relevant records. Also, the parties to a particular dispute may agree to exchange documents in advance of litigation in an effort to resolve their differences. More often than not, however, a lawsuit will likely be necessary before a company can demand disclosure from third parties. Government agencies can often compel disclosures prior to suit by using grand jury subpoenas and search warrants. The government's use of these investigative tools is very often the triggering event that prompts target companies to undertake their own internal investigations.

Grand jury subpoenas and search warrants

The government uses grand jury subpoenas to obtain relevant information to present to a grand jury for its return of an indictment. Companies served with grand jury subpoenas (or that become aware of the service on other parties of grand jury subpoenas focused on the company's activities) should retain outside counsel in order to best interface with the government, learn the government's intentions and, when necessary, negotiate to narrow the scope of the subpoena (as motions to quash grand jury subpoenas are rarely granted) and determine whether the government is seeking documents outside the United States. When companies respond to grand jury subpoenas, they should use the same document retention, production and review practices that they would use during internal investigations. See 'Document collection and review' above and section 4 'The duty to preserve evidence' below.

In US criminal investigations, the government may also, at any time, including early in its investigation, use search warrants to obtain company materials. Though search warrants are used far less frequently than grand jury subpoenas in investigations involving legitimate businesses, general

counsel should ensure that the company is prepared to respond to the execution of a search warrant.

Search warrants must be executed within the time specified thereon, but not more than 14 days after issuance, and during the day (unless expressly authorised for other times based on good cause) (Fed. R. Crim. Proc. 41(e)(2)). The officers also must provide the company with a copy of the warrant and an inventory and receipt of the items seized (id., (f)(1)).

General counsel should implement a set of procedures in case a warrant is served, which should include at least the following:

- inform outside counsel immediately so that she can be present and help guide the process;
- identify the areas the government is authorised to search and advise company counsel and/or the agents (or contact the US Attorney's Office or the judge who issued the warrant) if the agents are searching areas not permitted by the warrant;
- confirm that the inventory is a full and accurate record of what was seized;
- advise employees of their rights to consent to or to refuse government interview requests; and
- prepare the company for a review and analysis of the particular items seized and the potential reasons why.

Generally, all privileged documents should be clearly marked as privileged and company personnel and/or counsel should identify these documents to the agents executing the search warrant. These actions will not necessarily prevent the documents' seizure, but it is important to put the government on notice that it is seizing privileged materials. Federal agencies will often use so-called 'privilege' or 'taint' teams to filter out any potentially privileged materials. See USAM, 9-13.420. Alternatively, courts may appoint a lawyer to act as 'special master' to evaluate the responsiveness of the documents to the warrant (or valid exception to the warrant requirement), and any applicable privilege (or exception to its application). See, eg, *United States v Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995).

4. STEPS TO PRESERVE ASSETS/DOCUMENTS

The duty to preserve assets

In certain circumstances, companies may seek to prevent the use or transfer of assets allegedly held by third parties improperly. They can attempt to do so through asset freeze orders, which are sometimes available in private civil suits through preliminary injunctions or restraining orders. Although, in practice, such orders are rare in cases seeking monetary damages, US federal courts do have the inherent authority to issue them to ensure the availability of final relief (see *Reebok International Ltd v Marnatech Enterprises, Inc.*, 970 F.2d 552, 559 (9th Cir. 1992)), as well as statutory authority where explicitly authorised by underlying state or federal law (id., 558; Fed. Rul. Civ. Proc. § 64). Such freeze orders will enjoin conduct of the parties to the litigation (those who own or possess the property), their agents, employees and attorneys, and anyone else who participated in the questioned conduct

(Fed R. Civ. Proc. § 65; see also *FDIC v Faulkner*, 991 F.2d 262, 267 (5th Cir. 1993)), wherever they are located (*Steele v Bulova Watch Co.*, 344 US 280, 289 (1952)).

To issue a freeze order, the court must find either that the moving party will suffer irreparable injury and will probably prevail on the merits of the underlying claim or that *'serious questions are raised and the balance of hardships tips sharply in his favor'* (*Martin v International Olympic Committee*, 740 F.2d 670, 674–75 (9th Cir. 1984); cf. *United States v Odessa Union Warehouse Co-op*, 833 F.2d 172, 175 (9th Cir. 1987) (showing irreparable injury may not be required where the injunction is specifically authorised by statute and the statutory conditions are otherwise satisfied)). In practice, though, this is a high burden to meet. Inadmissible evidence may be used to support the order. See *Flynt Distributing Co. v Harvey*, 734 F.2d 1389, 1394 (9th Cir. 1984). Prior notice of a preliminary injunction must be given to the affected party, but a temporary restraining order can issue without notice provided certain conditions are met (Fed R. Civ. Proc. § 65).

The government can pursue companies' assets through criminal or civil forfeiture procedures. In criminal forfeiture, a defendant relinquishes to the government on conviction its legal interest in any property derived from or involved in the defendant's commission of various offences, including wire fraud, bank fraud and money laundering. See 18 U.S.C. § 982; 21 U.S.C. § 853. To accomplish forfeiture, the government is required to provide notice in the indictment that it will seek forfeiture of property (Fed R. Crim. Proc. 32.2(a)).

The government may, prior to forfeiture, seek a restraining order that restricts the transfer or use of the assets. It may do so either after charges are filed, or before the charges are filed so long as notice is given (21 U.S.C. § 853(e)(1); see also id., (e)(2) (temporary restraining order)). The court will grant this type of request only if it determines that there is a substantial probability that forfeiture will result and that the need to preserve the property outweighs any hardship to the affected parties (21 U.S.C. § 853(e)(1)). Alternatively, where a restraining order would not sufficiently preserve the property, a seizure order may be obtained (21 U.S.C. § 853(f)).

The government may also attempt forfeiture through civil process. This may be done administratively for certain types of property: contraband; anything used to transport contraband; personal property valued at less than $500,000; and monetary instruments of any value (18 U.S.C. § 983; 19 U.S.C. § 1607). The government must go through the court process to seize all other personal property and all real property (18 U.S.C. §§ 983, 985; 19 U.S.C. § 1607). Before forfeiting the property, the government can seize it with a seizure warrant or without one (ie 'freeze' it through a government order) if there is some exception to the usual warrant requirement, such as an exigent circumstance (18 U.S.C. § 981(b)(2)). Warrantless seizures are typically used in the case of bank accounts, where funds can be transferred easily.

The duty to preserve evidence

When counsel receives troubling information that reasonably causes her to evaluate whether the company should investigate further, she should immediately ensure that no potential evidence is destroyed. In certain circumstances she actually may have a duty to preserve evidence, which can result in serious consequences if she fails.

The duty to preserve company materials begins when a party reasonably anticipates litigation or a government investigation. See *Fujitsu Ltd v Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001); *Silvestri v General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) (citing *Kronisch v United States*, 150 F.3d 112, 126 (2d Cir. 1998)). It arises when a party *'has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation'* (*Zubulake v UBS Warburg LLC*, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003) (notice arising four months before lawsuit due to certain indications then that suit would be filed)).

When notice of a potential future litigation arises, company counsel should immediately suspend all routine document retention policies and issue what is known as a legal hold on all potentially relevant emails and documents. Counsel should identify and talk to key employees to ensure that they preserve all possibly relevant information. Counsel should also consider holding backup drives to protect the information.

The consequences of failing to adequately preserve documents can be serious. Prosecuting agencies may decline to give otherwise warranted cooperation credit. See USAM, 9-28.700. The destruction of evidence during or in anticipation of a government investigation could constitute obstruction of justice. See, eg, 18 U.S.C. § 1519. Courts may impose sanctions in some cases. See, eg, *Zubulake*, 219–20. For example, a court may allow a jury to draw an adverse inference against a party that destroyed evidence by concluding that such evidence would have been favorable to the other party. See id. (adverse inference sanctions are proper only when there is proof of bad faith or that the missing evidence would be favorable to the other party). Monetary sanctions also are available. See, eg, *in re: Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598 (D.N.J. 1997) ($1 million sanction).

5. CIVIL PROCEEDINGS

Company counsel should be familiar with the legal landscape in which an internal investigation is conducted. The remaining sections provide a non-exhaustive list of statutes and causes of action that are frequently the subject of government corporate prosecutions and internal investigations in the United States.

Trade secret theft

Private parties may rely on state trade secret laws to seek recovery for the theft of their property. Nearly every state has adopted the contents of the Uniform Trade Secrets Act (UTSA), published as amended in 1985 by the Uniform Law Commission, a non-profit, non-partisan legislative association.

Under the UTSA, misappropriation of trade secrets generally consists of the following: the knowing acquisition by improper means of a trade secret; or the unauthorised disclosure or use of a trade secret by someone who learned about it through improper means (UTSA § 1; see also, eg, Cal. Civ. Code § 3426.1–11).

In this context, 'improper means' includes *'theft … misrepresentation … or espionage …'* (UTSA § 1(1)). A 'trade secret' means *'information, including a … program, device … or process'* that is valuable because it is kept confidential and thus not publically known or ascertainable (id., § 1(4)).

Under the UTSA, either actual or threatened misappropriation may be enjoined (id., § 2). Damages may consist of actual losses and unjust enrichment, and may be recovered through a lump sum or royalty (id., § 3). Punitive damages of up to twice the compensatory damage amount may sometimes be awarded as well (id.). In-house counsel should ensure that claims are filed within the statute of limitations period.

It is important to observe here that trade secret theft is also criminalised under the Economic Espionage Act of 1996, and can involve significant penalties and prison time. See 18 U.S.C. §§ 1831–39, 3571 (maximum corporate penalty of $5 million; $250,000 fine for individuals and imprisonment for up to 10 years).

Fraud and embezzlement

To the extent a company's internal investigation uncovers that its employees harmed it through some form of deception, it may wish to pursue civil recovery under a fraud claim even when the government declines to pursue criminal charges. Generally speaking, although there is variation among the states, the state-level civil claim of fraud typically involves the following proof: a knowingly false representation or concealment of information done with the intention that it be relied on, inducing reasonable reliance and causing harm. See Restat. 2d of Torts § 525; see also, eg, Cal. Civ. Code §§ 1709–10; California Civil Jury Instruction No. 1900.

It is worth noting that state criminal fraud statutes typically do not require proof of reasonable reliance or resulting harm. See, eg, Cal. Pen. Code § 476; California Criminal Jury Instruction No. 1935 (cheque fraud requires proof of the defendant's knowing possession of a false cheque with intent to defraud). Companies and their employees may also be targeted by the federal government for a wide range of criminal activities under either the mail or wire fraud statutes. See 18 U.S.C. §§ 1341 (mail), 1343 (wire). These statues require the additional proof, among other things, that the defendant used mail or interstate wires (eg telephone or internet) to commit the fraud (id.; *Neder v United States*, 527 US 1, 25 (1999)). Penalties can be steep (18 U.S.C. §§ 1341, 1343, 3571): fines of up to $1 million and 30 years in prison if the crime affects a financial institution, or, for most other cases, a lesser fine and up to 20 years' imprisonment.

Embezzlement claims by companies against employees are also prevalent, and generally require proof that the employee took for his own benefit company property entrusted to him. See, eg, Cal. Pen. Code § 503; California

Criminal Jury Instruction No. 1806. Counsel should make sure to file any civil claims within the applicable statute of limitations period.

6. ANTI-BRIBERY/ANTI-CORRUPTION LEGISLATION

Anti-corruption statutes

The Foreign Corrupt Practices Act of 1977, as amended (FCPA), prohibits the payment of bribes to foreign officials in order to get or retain business, and is enforced by the DOJ and the US Securities and Exchange Commission (SEC). See 15 U.S.C. §§ 78dd-1 et seq. The FCPA also imposes certain record keeping and accounting restrictions on companies whose securities are listed in the US (so-called 'issuers') (15 U.S.C. § 78m).

The FCPA applies to a wide range of persons. Entities with a principal place of business in the US or organised under US laws, issuers and the directors, employees and stockholders acting for the above are subject to the FCPA (15 U.S.C. §§ 78dd-1, 78dd-2, 78dd-3). Citizens and residents of the US are covered anywhere in the world even if they are employees of foreign businesses not listed on US exchanges (id.). All foreign persons are subject to the FCPA whenever they or their agents are in the US (id.).

Entities may receive criminal fines of up to $2 million per bribery violation under the FCPA, while individuals can be fined up to $250,000 and imprisoned for a maximum of five years (15 U.S.C. §§ 78dd-2(g)(1)(A), 78dd-3(e)(1)(A), 78ff(c)(1)(A); 18 U.S.C. § 3571; see also A Resource Guide to the US Foreign Corrupt Practices Act, 68, available at *http://www.justice.gov/criminal/fraud/fcpa/guide.pdf* (FCPA Resource Guide)). For books and records violations, entities may be fined up to $25 million per violation, whereas individuals may receive up to $5 million in fines and imprisonment for up to 20 years (15 U.S.C. § 78ff(a); see also FCPA Resource Guide, 68).

Entities and individuals are subject to civil penalties of up to $16,000 per bribery violation (15 U.S.C. §§ 78dd-2(g), 78dd-3(e), 78ff(c); 17 C.F.R. § 201.1004; see also FCPA Resource Guide, 69). For books and records violations, defendants face penalties ranging from $7,500 to $150,000 for individuals and $75,000 to $725,000 for entities, or an amount up to the sum of their gain (15 U.S.C. § 78u(d)(3); 17 C.F.R. § 201.1004; see also FCPA Resource Guide, 69). Other consequences, such as debarment and loss of export privileges, are possible as well. See FCPA Resource Guide, 69–71. As with other violations of federal law, the SEC and DOJ are more likely to give credit to targets that make good-faith efforts at compliance. See, eg, FCPA Resource Guide, 29, 55–56, 59.

The DOJ also prosecutes bribery under various other federal anti-corruption statutes. See generally 18 U.S.C. §§ 201–27. For example, 18 U.S.C. § 201 criminalises the giving or offering of anything of value to a public official to influence any official act, and 18 U.S.C. § 215 proscribes similar conduct intended to corruptly influence an agent of a federally insured financial institution in connection with any transaction of that institution. A bribery conviction under section 201 can result in a fine of up to $250,000 ($500,000 for entities) or three times the value of the bribe and

15 years in prison (18 U.S.C. §§ 201, 3571). Convictions under section 215 involving more than $1,000 can result in a fine of up to $1 million or three times the value of the bribe and 30 years in prison (18 U.S.C. § 215).

Money laundering violations

The DOJ may also prosecute individuals and corporations for money laundering and currency transaction reporting violations. The Money Laundering Control Act of 1986 prohibits knowingly engaging in: transactions involving 'proceeds' from specified unlawful activity (including, for example, the proceeds of foreign official corruption) with the purpose of carrying on or concealing such unlawful activity or committing tax fraud (18 U.S.C. § 1956(a)), and any other transaction that involves 'proceeds' of more than $10,000 from specified unlawful activities (18 U.S.C. § 1957(a)). 'Proceeds' are *'property derived from or obtained or retained, directly or indirectly, through some form of unlawful activity, including the gross receipts of such activity'* (18 U.S.C. § 1956(c)(9)). A conviction of section 1956 can result in up to 20 years' imprisonment and fines of up to $500,000 or double the value of the property involved (18 U.S.C. § 1956(a)). Section 1957 convictions entail a maximum of 10 years in prison and fines of up to $250,000 ($500,000 for entities) or double the value of the property involved (18 U.S.C. §§ 1957(b), 3571).

The Bank Secrecy Act prohibits wilfully failing to file a currency transaction report for transactions exceeding $10,000 (31 U.S.C. § 5313; 31 C.F.R. § 1010.311). Civil liability can result in penalties of up to $100,000 (31 U.S.C. § 5321(a)). Criminal convictions entail fines of up to $250,000 and imprisonment for up to five years (31 U.S.C. § 5322). These limits are doubled for failures to file a required report while violating another law or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period (id.). The 'structuring' of transactions to avoid triggering a currency transaction report is also criminalised, and will result in fines of up to $250,000 ($500,000 for entities) and imprisonment for up to five years (31 U.S.C. § 5324; 18 U.S.C. § 3571). These limits are doubled for structuring while violating another law or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period (31 U.S.C. § 5324).