Reporting Employees' Criminal Activity

A Lexis Practice Advisor® Practice Note by Lesley Brovner and Mark Peters, Peters Brovner LLP

Lesley Brovner
Peters Brovner LLP

Mark Peters
Peters Brovner LLP

This practice note provides practical guidance regarding employers' reporting criminal activities of their employees to law enforcement.

Specifically, this practice note covers the following topics:

- Federal Reporting Requirements
- State General Criminal Reporting Requirements
- Potential Liability for Failure to Report and "Willful Blindness"
- Minimizing Risk and Liability through Internal Compliance Programs and Reporting
- Decreasing Risk of Claims Brought by Employees after Employers Report Their Alleged Crimes

As set forth below, there are limited circumstances under which employers are legally required to report illegal activities of their employees, depending on the specific law and/or jurisdiction. Even when not legally required, however, employers should contemplate whether to report based on ethical, business, and strategic considerations. This practice note also briefly discusses steps that employers can take to minimize their risk of liability via compliance programs and reporting.

While this Practice Note sets out some basic rules regarding the duty to report, this is a fact intensive—and evolving—issue and, before taking any action, employers should consult with an attorney and review the matter in light of the specific facts at hand.

For an overview of the law and legal standards governing the imposition of criminal liability on officers, directors, and corporations for the acts of employees, see Corporations, Directors, and Officers: Potential Criminal and Civil Liability. For practical guidance on various steps that in-house and outside counsel should take when representing a company in a government investigation of a senior executive, see Government Investigations of Senior Executives Checklist: Employer Considerations.

For guidance on disciplining employees, see Disciplining Employees: Key Considerations. For a checklist on disciplining employees, see Disciplining Employees: Best Practices Checklist. For guidance on disciplining unionized employees, see Disciplining and Investigating Union Employees. For more information on discipline generally, see the practical guidance in Investigations, Discipline, and Termination — Discipline.

For recent key Labor & Employment legal developments that may impact this content, see the Labor & Employment Key Legal Development Tracker.

Federal Reporting Requirements

This section provides guidance on reporting employees' violations of various key federal laws.

Duty to Report Employees Who Access Child Pornography

While the statutory contours of an employer's duty to report an employee who uses company technology to view child pornography are not fully clear in some cases, it appears that a duty to report will likely be implied broadly.

Determining Whether an Employer is an "Electronic Communication Service Provider" with a Reporting Duty

To reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children, 18 U.S.C. § 2258A specifically requires that "electronic communication service providers" or "remote service providers" report child pornography to the CyberTipline operated by the National Center for Missing and Exploited Children. 18 U.S.C. § 2258E.

The section expressly uses the definition of "electronic communications service (ECS)" from the Stored Communications Act (SCA). 18 U.S.C. § 2711. The SCA, in turn, defines electronic communications service as "any service which provides to users the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

The penalties for failing to report can be significant. Under 18 U.S.C. § 2258(A)(e), a provider that knowingly and willfully fails to make a required report shall be fined up to $150,000 for its first violation, and up to $300,000 for any second or subsequent knowing and willful failure. 18 U.S.C. § 2258A(e).

It is not clear whether any employer who provides its employees with internet service or email would be considered an electronic communications service (ECS) provider, and thus obligated to report. In the context of the SCA, courts have held that ECS providers include telecommunications companies such as Arch Wireless, internet providers such as AOL, and social networking companies such as Facebook. See, e.g., Quon v. Arch Wireless, 929 F.3d 892, 903 (9th Cir. 2008), rev'd on other grounds, 560 U.S. 746 (2010) (Arch Wireless); Freedman v. America Online, 325 F. Supp. 2d 638, 644 n.4 (E.D. Va. 2004) (AOL); In re 381 Search Warrants, 29 N.Y.3d 231 (2017).

We are not aware of any federal court that has found that an employer-provided internet constitutes an ECS provider. However, one court has held that a college's email server provided to students did constitute an ECS provider. Hately v. Watts, 917 F.3d 770, 788 (4th Cir. 2019). As such, caution should be exercised before assuming that an employer's computer systems will not, under any circumstances, be covered. See also Legal Analysis: Practice Tips: What To Do When Your Client Discovers Child Pornography On Workplace Computers, 56 B.B.J. 12 (Summer 2012) ("On its face, the statute appears to apply its mandatory reporting requirement to any employer that provides e-mail access to its employees.").

For more guidance on the SCA, see Stored Communications Act (SCA): Practical Considerations.

Potential Common Law Employer Duty to Report Child Sexual Exploitation

Even outside of the question of whether an employer is an electronic service provider, at least one court has found a common law duty to report child sexual exploitation. In Doe v. XYC Corporation, 382 N.J. Super. 122, 140–43 (Super. Ct. App. Div. 2005), the court held that an employer that is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. In noting there was a duty to report the employee's conduct to the authorities, the court noted that it is a crime, both state and federal, to possess or view child pornography, N.J. Stat. Ann. § 2C:24-4(b)(5)(b); 18 U.S.C. § 2252, § 2256(8)(B). Doe, 382 N.J. Super. at 141. However, the court expressly declined to determine whether the corporation was an electronic communications server under 18 U.S.C. § 2510(15). Doe, 382 N.J. Super. at 141, n. 3.

Monitoring Electronic Devices at Work

While there may be a duty to report once the employer becomes aware of potentially prohibited conduct, there does not appear to be a duty to monitor initially. 18 U.S.C. § 2258A(f). That said, employers should do what they can to prevent anyone from using their equipment in the commission of a crime.

Toward that end, the employer should have policies stating the following:

- Any employer-issued equipment remains the property of the employer.

- Employees have no right to privacy with respect to employer-owned equipment.
- The employer may access and search the equipment at any time and without notice.

Ideally, employers should remind employees of their lack of privacy interest each time they log on to their computers. Employers should also develop policies regarding employee-owned equipment used for employer business or that the employer's IT department services. In other words, employers should inform employees that if they wish to use personal devices for work purposes, those personal devices will be subject to the same search conditions as employer-provided equipment. There are two benefits to such a policy. First, stating that monitoring will occur eliminates concerns about violation of privacy. Second, where employees are aware that monitoring is occurring, that very awareness acts as a deterrent of bad behavior.

Employers should also engage in the following additional best practices to minimize the possibility that employees will access child pornography at work:

- Block certain sites from all work computers.
- Set up alerts with certain key words so that if employees seek out sites with those key words, supervisors are notified.
- Consider subscribing to a service that blacklists pornography sites as they are created.
- Conduct periodic audits of their employees' internet use. This can be more easily accomplished if the employer centralizes all internet traffic through a proxy server.

For more information on drafting a communications systems, email, networks, and internet policy, see Communications System, E-mail, Network, and Internet Policies: Key Drafting Tips and Communications Systems, Email, Networks, and Internet Policies Checklist. For a model policy, see Communications Systems, Email, Networks, and Internet Policy; see also Communications Systems, E-mail, Networks, and Internet Policy Acknowledgment.

For information on policies governing electronic devices in the workplace, see Computer, Mobile Phone, and Other Electronic Device Policies: Key Drafting Tips and Bring-Your-Own-Device (BYOD) Policies: Key Drafting Tips. For an electronic device policy acknowledgment form, see Computers, Mobile Phones, and Other Electronic Devices Policy Acknowledgment. For an electronic device policy, see Computers, Mobile Phones, and Other Electronic Devices Policy. For a form governing personal electronic devices in the workplace, see Bring Your Own Device (BYOD) Policy.

Reporting SEC Violations

The Securities and Exchange Act of 1934 (the Exchange Act entrusts the Securities Exchange Commission (SEC) with broad authority over all aspects of the securities industry, including the power to register, regulate, and oversee brokerage firms, transfer agents, and clearing agencies. The Exchange Act also identifies and prohibits certain types of conduct in the markets and provides the SEC with disciplinary powers over regulated entities and persons associated with them.

Common violations that may lead to SEC investigations include:

- Misrepresentation or omission of important information about securities
- Manipulating the market prices of securities
- Stealing customers' funds or securities
- Violating broker-dealers' responsibility to treat customers fairly
- Insider trading (violating a trust relationship by trading on material, non-public information about a security) –and–
- Selling unregistered securities

See How Investigations Work.

In addition, the Exchange Act legally protects employee whistleblowers. 15 U.S.C. § 78u-6; 17 C.F.R. § 240.21F-2. See Whistleblower Reporting: Training Presentation. The public, self-regulatory organizations, and other entities may initiate complaints. See Tips, Complaints, and Referrals, 2.2. Violators of the Exchange Act can be subject to criminal prosecution.

Best Practices

While there is no express requirement that an entity disclose prohibited employee misconduct to the SEC, several rules suggest that such reporting is an important best practice, especially for broker dealers.

The Exchange Act imposes a duty on broker dealers to supervise their employees to ensure that those individual employees do not violate the various securities laws. As the SEC explained in a publication providing guidance on this topic:

> Section 15(b)(6) of the Exchange Act authorizes the Commission to institute proceedings against a natural person associated with a broker-dealer if someone under that person's supervision violates the provisions of the federal securities laws, the Commodity Exchange Act, the rules or regulations under those statutes, or the rules

of the Municipal Securities Rulemaking Board, and the supervisor failed reasonably to supervise that person with a view to preventing the particular violation.

In this regard, compliance and legal personnel should inform direct supervisors of business line employees about conduct that raises red flags and continue to follow up in situations where misconduct may have occurred to help ensure that a proper response to an issue is implemented by business line supervisors. Compliance and legal personnel may need to escalate situations to persons of higher authority if they determine that concerns have not been addressed.

Frequently Asked Questions about Liability of Compliance and Legal Personnel at Broker-Dealers under Sections 15(b)(4) and 15(b)(6) of the Exchange Act, Division of Trading and Markets (Sept. 30, 2013).

While the above language does not specifically require self-reporting to the SEC or law enforcement, it is hard to read this guidance without assuming that such reporting, in appropriate instances, may be expected.

In this context, it is important to also note the affirmative benefit to an entity for voluntarily reporting an employee's criminal conduct. As set forth in a 2001 SEC report (known as the Seaboard Report), the SEC took no action against a company whose employee caused the parent company's books and records to be inaccurate and its periodic reports misstated, and then covered up those facts. In this instance, the company's self-reporting was a factor in the SEC's decision to not take action. See SECURITIES EXCHANGE ACT OF 1934 Release No. 44969 / October 23, 2001 ACCOUNTING AND AUDITING ENFORCEMENT Release No. 1470 / October 23, 2001.

In the Seaboard Report, the SEC identified various criteria to consider in determining, on a case-by-case basis, whether, and how much, to credit a company's self-policing, self-reporting, remediation, and cooperation. Some of these considerations include:

- The nature of the misconduct involved
- How the misconduct arose
- Where in the organization the misconduct occurred
- How long the misconduct lasted
- How much harm has the misconduct inflicted upon investors and other corporate constituencies
- How was the misconduct detected and who uncovered it
- How long after discovery of the misconduct it took to implement an effective response
- The steps the company took upon learning of the misconduct
- The processes the company followed to resolve these issues and ferret out necessary information, and whether it did a thorough review of the nature, extent, origins, and consequences of the conduct and related behavior
- Whether the company promptly made available to SEC staff the results of its review and provided sufficient documentation reflecting its response to the situation

See SECURITIES EXCHANGE ACT OF 1934 Release No. 44969 / October 23, 2001 ACCOUNTING AND AUDITING ENFORCEMENT Release No. 1470 / October 23, 2001.

Thus, while employers are not explicitly required by the Exchange Act to disclose prohibited employee misconduct to the SEC, reporting is a best practice that should be seriously considered following an analysis of the foregoing factors.

Financial Industry Regulatory Authority (FINRA)

Regardless of whether an employer chooses to report its employee's illegal activities to the SEC, it may still be required to report such activities to the Financial Industry Regulatory Authority (FINRA), an independent regulator of securities firms in the United States. Member firms are required to report a wide variety of violations to FINRA.

For example, FINRA Rule 4530(b) states that "each member firm shall promptly report to FINRA, but in any event not later than 30 calendar days, after the firm has concluded or reasonably should have concluded that an associated person of the firm or the firm itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization (SRO)."

However, employers need not report all violative conduct, but only conduct that has or may have widespread impact on the member, its customers, or the markets, or that arises from a material failure of the firm's systems, policies, or practices involving numerous customers, multiple errors, or significant amounts of money. See Broker-Dealer Disclosure and Complaint Filings: FINRA Rule 4530; see also Rule 4530 Frequently Asked Questions (Answer to Question 1.1 (Are member firms required to report internal conclusions of all rule violations under FINRA Rule 4530(b)?).

FINRA may impose sanctions for failing to report or filing false, misleading, or inaccurate reports, including fines ranging from $5,000 to $146,000, disgorgement of any gain, and suspending the responsible principal in all supervisory

capacities for 10 to 30 business days. Moreover, for serious cases, FINRA has the authority to suspend the firm's membership until it corrects the deficiency, suspend the responsible principal for up to two years, or bar the principal in all supervisory capacities. FINRA's Sanctions Guidelines (March 2019) are available here.

Finally, member firms may receive reduced sanctions by (1) self-reporting violations by providing a detailed account of the conduct and offering to provide additional explanation, documents, and witnesses, (2) taking extraordinary actions to correct deficiencies and provide remedies to customers, and (3) providing substantial assistance to FINRA investigations.

For more information on FINRA's reporting requirements, see Broker-Dealer Disclosure and Complaint Filings: FINRA Rule 4530.

Reporting Wage and Hour Violations

Section 216 of the Fair Labor Standards Act (FLSA), 29 U.S.C. § 203 et. seq., provides:

> Any person who willfully violates any of the provisions of section 215 of this title shall upon conviction thereof be subject to a fine of not more than $10,000, or to imprisonment for not more than six months, or both.

29 U.S.C. § 216.

Section 215, in turn, references various federal wage and hour law requirements, including employers' obligation to pay minimum wage and overtime. 29 U.S.C. § 215.

Discovery of wrongdoing is often made through agency investigators or the employee-whistleblowers whom FLSA protects from retaliation under 29 U.S.C. § 215(a)(3). Sometimes employers find out on their own through self-audits or other means that an employee has willfully violated the FLSA.

Rules also exist for reporting inadvertent violations of the FLSA. However, employers should consider whether to report violations to the Department of Labor's Wage and Hour Division. The DOL's Payroll Audit Independent Determination (PAID) program facilitates resolution of some potential overtime and minimum wage violations under the FLSA. The program's primary objectives are:

- To resolve such claims expeditiously and without litigation
- To improve eligible employers' compliance with overtime and minimum wage obligations –and–
- To ensure that more employees receive the back wages they are owed and more quickly

Under the PAID program, eligible employers audit their compensation practices for potentially non-compliant practices. Once an employer identifies any potential claims it wants to resolve, the employer must then:

- Specifically identify the potential violations
- Identify which employees were affected
- Identify the timeframes in which each employee was affected –and–
- Calculate the amount of back wages the employer believes are owed to each employee

Whether to participate in the PAID program requires a balancing of various factors. On the one hand, participation in the program could eliminate the risk of double damages and costly litigation. On the other hand, participation could subject the employer to a broader investigation than anticipated or one or more follow up investigations—and does not resolve potential state law wage and hour claims. Thus, employers should proceed with caution.

For detailed guidance on the PAID program, including whether to participate in the program, see the subsections entitled "Payroll Audit Independent Determination (PAID) Program" and "Employers' Considerations for Whether to Participate in the PAID Program" in Settlements and Resolutions of FLSA Claims and Potential FLSA Violations.

Workplace Violence and the OSH Act's General Duty Clause and Guidelines

Section 5(a)(1) of the Occupational Safety and Health Act of 1970—the General Duty Clause—requires employers to provide their employees with a place of employment that is "free from recognized hazards that are causing or are likely to cause death or serious physical harm."

According to Occupational Safety and Health Administration (OSHA),

> The courts have interpreted OSHA's general duty clause to mean that an employer has a legal obligation to provide a workplace free of conditions or activities that either the employer or industry recognizes as hazardous and that cause, or are likely to cause, death or serious physical harm to employees when there is a feasible method to abate the hazard.

See OSHA Workplace Violence Fact Sheet.

Notwithstanding this obligation, OSHA does not appear to specifically require employers to report incidents of workplace violence to law enforcement.

Best Practices

While there is no express self-reporting requirement regarding workplace violence, OSHA does list some best practices which include:

- Assigning responsibility and authority for the various aspects of the workplace violence prevention program to ensure that all managers and supervisors understand their obligations
- Maintaining a system of accountability for involved managers, supervisors and workers
- Establishing policies that ensure the reporting, recording, and monitoring of incidents and near misses and that no reprisals are made against anyone who does so in good faith
- Determine who needs to be notified, both within the organization and outside (e.g., authorities), when there is an incident
- Understand what types of incidents must be reported, and what information needs to be included
- Develop a standard response action plan for violent situations, including the availability of assistance, response to alarm systems and communication procedures
- As part of their overall program, employers should evaluate their safety and security measures.
    - Top management should review the program regularly and, with each incident, to evaluate its success.
    - Responsible parties (including managers, supervisors and employees) should reevaluate policies and procedures on a regular basis to identify deficiencies and take corrective action.

See OSHA Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers.

As these guidelines suggest, reporting workplace violence—if not mandatory—is certainly a best practice. Indeed, given the OSH Act's requirements that employers maintain a "workplace free of conditions or activities … that cause, or are likely to cause, death or serious physical harm to employees when there is a feasible method to abate the hazard," reporting such criminal "conditions or activities" may be one of the best ways to remove the hazard and keep the workplace safe. For example, employers clearly should report to the police an active shooter situation, hopefully in time to protect their employees.

Employers should also investigate claims of other types of violence in the workplace, such as an allegation of rape by one employee against another, and take remedial measures to protect and support the alleged victim. For example, prior to the conclusion of its investigation, the employer could suspend the alleged perpetrator with pay (so as to remove the employee from the workplace) and assist and/or cooperate with any criminal investigation initiated by the alleged victim. Should the allegations be deemed credible following investigation, the employer could terminate the perpetrator's employment for cause.

If an OSHA inspector learns of workplace violence, they will likely report such an incident to the relevant authorities. See, e.g., OSHA Directive No. 01-02-058. Employers should self-report such an incident to the authorities when the employer learns of it, rather than being forced to explain the failure to do so after the fact.

For more information, on handling workplace violence incidents, see Workplace Violence: Key Legal Issues, Prevention, and Response.

For more information on OSHA, including OSHA reporting requirements and the General Duty Clause, see OSH Act Requirements, Inspections, Citations, and Defenses.

State General Criminal Reporting Requirements

Some states have statutes requiring individuals or corporations to report crimes. For example, in Colorado "[i]t is the duty of every corporation or person who has reasonable grounds to believe that a crime has been committed to report promptly the suspected crime to law enforcement authorities." Colo. Rev. Stat. § 18-8-115. In Texas, a "person commits an offense if the person observes the commission of a felony under circumstances in which a reasonable person would believe that an offense had been committed in which serious bodily injury or death may have resulted." Tex. Penal Code § 38.171 (Failure to Report Felony).

New York

New York has no general criminal reporting requirement. However, state statutes require reporting to authorities in limited instances. New York state mandates reporting to the New York State Central Register (SCR) of Child Abuse and Maltreatment only by certain individuals who have a reasonable suspicion of child abuse by a parent or legal guardian. N.Y. Soc. Serv. Law §§ 413, 415. Mandated reporters fall into five categories of providers: health care, human services, childcare, education, and law enforcement.

While an employer that does not fall into one of these categories is not obligated to report child abuse, such reporting is clearly a best practice in any event. Indeed, New

York law expressly states that non-mandated reporters may make such reports and are provided immunity from liability for making such reports in good faith. N.Y. Soc. Serv. L. Sections 414, 419.

If a call to the SCR provides information about an immediate threat to a child or a crime committed against a child, but the perpetrator is not a parent or other person legally responsible for the child, the SCR staff will make a Law Enforcement Referral (LER). The relevant information will be recorded and transmitted to the New York State Police Information Network or to the New York City Special Victims Liaison Unit. This is not a Child Protective Service (CPS) report, and local CPS will not be involved.

While every state similarly provides for mandatory reporting of child abuse, the specifics vary by state. See Mandatory Reporters of Child Abuse and Neglect. Institutional obligations similarly vary by state.

Potential Liability for Failure to Report and "Willful Blindness"

As noted above, there are some instances where there is an obligation to report and thus penalties for failing to do so. In this regard, it is important to understand that the "willful blindness" doctrine may impose an obligation to report whenever a reasonable person would suspect improper conduct and chooses to deliberately remain ignorant of the facts at hand.

Courts have imposed the willful blindness rule in both criminal and civil contexts. In the criminal context, one court has explained the rule as follows:

> Defendants cannot escape the reach of these statutes by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances. Defendants who behave in this manner are just as culpable as those who have actual knowledge. Persons who know enough to blind themselves to direct proof of critical facts in effect have actual knowledge of those facts.

United States v. Marsh, 820 F. Supp. 2d 320, 335 (E.D.N.Y. 2011) (quoting Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2070 (2011)).

In the context of civil fraud, the rule is virtually the same:

> A person acts with willful blindness when he or she subjectively believed that there was a high probability that a particular fact exists and took deliberate actions to avoid learning of that fact.

On Site Energy Co. v. MTU Onsite Energy Corp., 2013 U.S. Dist. LEXIS 109009, at *14 (E.D.N.Y. Aug. 2, 2013) (approving the above as a jury instruction).

Finally, in the more general context of civil litigation—here, an intellectual property case—the Second Circuit has explained that: "To be willfully blind, a person must suspect wrongdoing and deliberately fail to investigate." Tiffany Inc. v. Ebay Inc., 600 F.3d 93, 109 (2d Cir. 2010).

Thus, regardless of whether the duty to report involves criminal or civil actions, where an employer suspects, or should suspect, that reportable activity has occurred, the employer cannot simply turn a blind eye or fail to make reasonable inquiries.

Minimizing Risk and Liability through Internal Compliance Programs and Reporting

The first step in minimizing risk and liability is to have a robust compliance program, even for small companies. To prevent and detect violations of laws and regulations, companies should:

- Assess the risks that the company needs to address
- Implement written policies, procedures, and standards of conduct including an employee handbook
- Designate a compliance officer and compliance committee
- Conduct training and education on the company's policies, procedures, and standards of conduct
- Develop a means of reporting violations to the compliance officer or committee
- Have a clear policy that precludes retaliation for such reporting
- Conduct internal monitoring and auditing of compliance with policies, procedures, and standards of conduct
- Enforce policies, procedures, and standards of conduct through well-publicized disciplinary guidelines
- Provide for due process protections for suspected wrongdoers
    - This is important because such procedures will provide an employer with some protection if the employee whose conduct is reported chooses to object to his or her treatment.
- Respond promptly to detected offenses and undertake corrective action

As to the final bullet point, where a robust compliance program reveals conduct of the type described in the prior sections of this practice note, employers may need to report the conduct. Even where the law does not mandate reporting the conduct, it may be advisable to report it to minimize the risk that the relevant regulators will consider the employer in question to be culpable for the bad acts when (as is almost always the case) they eventually come to light. Such self-reporting will provide significant good will with both law enforcement and regulatory agencies.

For guidance on drafting employee codes of conduct policies, see Employee Codes of Conduct: Key Drafting Tips. For sample employee codes of conduct, see Code of Conduct and Ethics and Whistleblowing Policy. See also Principal Executive and Senior Financial Officers Code of Ethics.

Decreasing Risk of Claims Brought by Employees after Employers Report Their Alleged Crimes

Reporting (suspected) criminal activity of employees—whether required by law or voluntarily—is not without risk. Indeed, employers who accuse employees of criminal activity or suspected criminal activity may be subject to claims by the accused employees, including defamation and discrimination. To mitigate that risk, consider the following practical strategies:

- **Conduct a thorough investigation.** An employer that suspects that one or more of its employees have engaged in criminal activity should conduct a thorough investigation to determine whether criminal activity has occurred and by whom. Depending on the size, scope, seriousness, and nature of the matter, employers should launch either an internal investigation led by inhouse house or an external investigation led by outside counsel. If the suspected crimes are financial in nature, the employer should also consider engaging and utilizing relevant experts, such as forensic accountants and auditors, to help determine the facts and guide strategy. Conducting a fair and thorough investigation establishing that the employee engaged (or likely engaged) in criminal activity will help the employer defend against claims that it discriminated against or defamed the employee.

  For practical guidance on how to conduct an effective workplace investigation, see Workplace Investigations: Step-by-Step Guidance. For practical guidance on various steps that in-house and outside counsel should take when representing a company in a government investigation of a senior executive, see Government Investigations of Senior Executives Checklist: Employer Considerations. For practical guidance to help limit defamation claim exposure, see Defamation Basics in Employment Law and Confidentiality in Workplace Investigations.

- **Keep a paper trail and prepare investigation memo.** The Company should also prepare and maintain documentation regarding the steps it took during the investigation as well as the facts discovered. As mentioned above, fairness and thoroughness in the investigative process should help provide a defense to claims of discrimination and defamation. For best practices on documenting workplace investigations, see Documenting Key Events in Workplace Investigations.

- **Workplace violence or threatened violence may require immediate action.** If the suspected criminal activity involves actual or threatened harm to the health and safety of employees, such as an employee using, brandishing, or threatening to use a weapon at the workplace, the employer should take immediate action (such as calling 911 or otherwise contacting the police) regardless of the status of its investigation. For practical guidance on legal issues related to workplace violence and strategies for preventing and responding to workplace violence, see Workplace Violence: Key Legal Issues, Prevention, and Response and Workplace Violence Prevention Checklist. For information on drafting workplace violence policies, see Workplace Violence Policies: Key Drafting Tips and Workplace Violence Policy.

- **Preserve documents.** Immediately upon learning of potential illegal activity, take steps to preserve both paper and electronic documents so that they cannot be destroyed or altered.

Lesley Brovner, Partner, Peters Brovner LLP

Prior to co-founding Peters Brovner, Lesley Brovner served as First Deputy Commissioner of the New York City Department of Investigation (DOI) from 2014 to 2018. While in this role, Ms. Brovner directed complex criminal and civil investigations, oversaw the issuance of all agency reports and supervised DOI's counsel's office.

As First Deputy Commissioner, Ms. Brovner worked on a regular basis with senior prosecutors and regulators at numerous city and state agencies. This work resulted in the prosecutions of corporations and nonprofits that engaged in fraudulent activity as well as city workers involved in a variety of corrupt schemes. Ms. Brovner personally directed several major investigations, including:

DOI's year-long examination into the NYPD's failure to properly investigate sexual assault. The investigation resulted in City Council legislation requiring changes in NYPD practices.

DOI's Investigation into the City's sale of Rivington House and whether the sale of that non-profit AIDS hospice was mismanaged or otherwise improperly influenced by contributors to the Mayor's political campaign.

Multiple investigations of construction fatalities and other illegal conduct on construction sites. These investigations included work with the Construction Fraud Task Force which was jointly run by several of the City's District Attorneys and DOI.

Prior to working at DOI, Ms. Brovner was a prosecutor for almost two decades at the New York State Attorney General's Office and the Queens District Attorney's Office. During that time she prosecuted numerous matters, including: political corruption, consumer fraud, tax fraud, antitrust violations, social security fraud and the unlicensed practice of nursing and medicine. Ms. Brovner also has extensive appellate experience including before the New York State Court of Appeals. Finally, Ms. Brovner served as the Chief Compliance Officer for the New York State Liquidation Bureau.

Mark G. Peters, Partner, Peters Brovner LLP

Prior to co-founding Peters Brovner, Mark Peters served as Commissioner of the New York City Department of Investigation (DOI) from 2014 to 2018. While in this role, Mr. Peters supervised the 700-person law enforcement agency responsible for investigating corruption, waste, fraud and abuse by city agencies, city workers and private entities that do business with the city.