KOBRE & KIM | DISPUTES AND INVESTIGATIONS

Kobre & Kim's Special Investigations Team

Adriana Riviere-Badell
Miami
adriana.riviere-badell@kobrekim.com

Jonathan D. Cogan
New York
jonathan.cogan@kobrekim.com

Matthew I. Menchel
Miami
matthew.menchel@kobrekim.com

Michael Keilty
New York
michael.keilty@kobrekim.com

Nicholas Surmacz
London
nicholas.surmacz@kobrekim.co.uk

Steven G. Kobre
steven.kobre@kobrekim.com

SEPTEMBER 26, 2024

The Next Challenge For Independent Outside Counsel Performing Internal Investigations: Employees' Personal Cell Phones

The private cell phones of employees in high-stakes internal investigations can pose a serious challenge for general counsels or institutional law firms who do not have the independence to obtain these devices and require their review. In these complex situations, an independent, "one-off" third party firm uninterested in pursuing institutional relationships can be critical in delivering an unbiased, confidential assessment. Below we share a few perspectives on how to mitigate risks.

The private cell phones of employees in high-stakes internal investigations can pose a serious challenge for general counsels or institutional law firms who do not have the independence to obtain these devices and require their review. In these complex situations, an independent, "one-off" third party firm uninterested in pursuing institutional relationships can be critical in delivering an unbiased, confidential assessment.

Recent experience shows a high-stakes risk for companies: The role of employees' personal devices for work-related communications. Employees are increasingly using their personal devices to discuss work-related topics. Employers and employees are uncertain of their rights and responsibilities, especially as new regulations and enforcement actions can lead to expensive and disruptive government investigations or civil litigation. As it becomes a burgeoning matter, companies can access the right investigative tools and take preventive measures to undercut emboldened regulators like the U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) looking to find violations.

Companies have been forced to confront company-related information their employees share on apps such as iMessage, Snapchat, Signal, WhatsApp, Telegram, Viber, Line, and WeChat. Many employees use these apps on their personal phones under the belief that they are private devices and beyond the reach of their employers. Despite this belief, the U.S. Government, civil litigators, and companies performing internal investigations often have effectively obtained and searched the information on their personal devices.

Because personal cell phones can potentially contain relevant information, companies have now found themselves subject to various rules regarding the preservation of information on employees' personal phones. The SEC and CFTC recently announced settlements totaling nearly US $474 million with several broker-dealers, investment advisers, and other registered firms over failures to maintain and preserve text messages and other electronic communications as required under U.S. federal law.

How Companies Can Mitigate Risks

Companies should thus seek to limit liability by taking some of the following preventive measures to avoid serious risks associated with investigations:

1. **Be Clear.** Companies should draft comprehensive policies and provide clear instructions and training on what employees are and are not allowed to communicate on electronic devices and messaging apps, especially when engaging in work-related communications via personal devices.
2. **Be Prepared.** Companies should consider expressly including the company's right of access to personal devices used for business purposes in employment contracts and manuals. Doing so could allow access to certain documents contained on those devices for legal purposes. It may also significantly decrease the time and cost burden involved in giving disclosure in any investigation or litigation to which the company is subject.
3. **Be Proactive.** In addition to considering providing company-owned devices to employees, companies should monitor internal systems for indicators that employees may be using unauthorized devices or applications for business purposes. Companies should run searches through company communications for keywords and phrases, such as names of prohibited applications, and maintain a log of employees using personal devices for business purposes. This approach can help companies identify potential employee violations. To facilitate enforcement, companies should run regular audits, explain what "business" communications mean, and notify employees that the company reserves the right to access communications on personal devices if concerned about an employee's violation. Companies that are required by regulation to maintain business communications should consider banning the use of certain apps for business purposes or certain app functions that automatically delete messages. Apps like Snapchat, WhatsApp, and Telegram include functions that could result in such deletions of business communications.
4. **Know the Rules.** Companies should know the rules regarding maintaining electronic communications and those involving employers' and employees' privacy and regarding surveillance of communication devices.
5. **Establish a Plan**. Employers and their counsel should have a plan for obtaining business information from employees' personal devices. For example, some companies have lists of counsel who are (a) available to represent pools of employees, (b) can confidentially search employees' personal devices as counsel to the employees, and (c) produce to the company business-related communications. This mechanism has allowed companies to obtain business-related information from employees' cell phones without the employer viewing or accessing personal, non-business-related information on employees' devices.

Companies and their incumbent legal counsel have to deal with a challenging landscape: U.S. regulators are taking increasingly aggressive positions against companies that fail to monitor for communications on both company and personal devices. Obtaining such information on personal devices is viewed by employees as intrusive as they do not want their employer viewing their personal data. Counsel conducting investigations need to balance these concerns with the desire of regulators to obtain information relevant to their business. This balance is best achieved by lawyers who can provide clear-headed assessments informed by a deep familiarity with regulators' authority and reach while avoiding concern that obtaining cell phone data will negatively impact their long term institutional relationship with their client.

About Kobre & Kim

Kobre & Kim is a conflict-free global law firm focusing on cross-border disputes and investigations, often involving fraud and misconduct.

Our team:

- Is frequently called upon to work alongside a client's regular outside legal counsel in conducting independent investigations on behalf of boards of directors, audit committees and multinational corporations in matters involving various stakeholders where credibility and independence are required.
- Focuses exclusively on serving as special counsel in investigations matters and typically does not pursue institutional relationships.
- Delivers independent assessments in complex situations, affording a high level of comfort about our confidentiality due to a lack of ties with other industry participants.
- Has an in-depth understanding of varying attorney-client privilege laws, country-specific data protection laws and employment laws, and other special issues that arise in high-stakes investigations.
- Is able to either advocate directly or to work cooperatively with local counsel, in jurisdictions in the U.S., UK, EMEA, Asia, Latin America and key offshore financial centers.