LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, MAY 11, 2021

PERSPECTIVE

Employee charged with COVID relief fraud? Questions for GCs

By Byron J. McLain and Hawwi Edao

The U.S. Department of Justice already has publicly charged almost 500 defendants with criminal offenses based on fraud schemes connected to the COVID-19 pandemic. Unfortunately, these prosecutions can have unintended consequences on unsuspecting businesses, as many of these accused individuals actually work as employees for uninvolved companies. As employees, they may have utilized their access to confidential employee or client information at work to create the allegedly fraudulent business applications to the government for COVID-19 relief. The unsuspecting, uninvolved victim companies may receive a subpoena or interview request from the government for additional investigative information against their accused employees. As a result, general counsel at companies need to balance the instinct to cooperate with the government against subjecting a company's confidential business interests to further unnecessary intrusion.

On March 11, President Joe Biden signed the American Rescue Plan Act into law. This new relief package provides additional pandemic support for legitimate businesses. As the payment of PPP loans and other COVID-19 relief from the government increases, the government is very likely to charge many more people for abusing the government programs' funds. The DOJ already has developed key criminal and civil enforcement measures to combat PPP loan fraud in particular. In the event a company's employee is accused of committing COVID-19 relief fraud, general counsel should consider now their response to the possibility of a government investigation. Specifically, general counsel at least need to be able to answer these three questions:

General counsel at companies need to balance the instinct to cooperate with the government against subjecting a company's confidential business interests to further unnecessary intrusion.

1. Was any company employees' or clients' private data implicated in the alleged fraud?
2. What level of cooperation should the company provide with the federal investigation into the criminal allegations?
3. How should the company treat the accused employee's job status during the course of the investigation?

Question 1: Was any company employees' or clients' private data implicated?

Consider the following hypothetical: The general counsel at Regions Corporation gets a late-night call from the company's Human Resources Department. One of the company's salespeople, Michael Henobetter, was just arrested for bank fraud by the FBI. The general counsel was astonished and worried. First, she knew Michael personally. He was an all-star salesperson at the company with great potential. Second, the general counsel knew that Michael had access to the personal information of the company's clients as part of his work in the Sales Department, and the company's confidential data could have been compromised in the alleged fraud.

Like most companies, Regions Corporation stores massive amounts of employee and client data on its computers, cloud-based servers, and internet applications. As a result, when a company's employee is the target of a COVID-19 relief fraud investigation, in-house counsel must quickly assess whether any sensitive information for the company's employees or clients was compromised. As a result, the company should forensically investigate any company-owned devices utilized by the accused employee. A company can access and retrieve employee data (i.e., emails, documents, text messages, etc.) stored on company systems and devices if the company establishes that the employer has common authority and access to such information. The U.S. Supreme Court, in *City of Ontario v. Quon*, upheld the search of an employee's company-owned electronic device where there was "a legitimate work-related rationale" for the search by the employer. 560 U.S. 746, 761 (2010); see also *Holmes v. Petrovich Dev. Co., LLC*, 191 Cal. App. 4th 1047, 1071 (2011) (employee's email communications on her work computer to her personal attorney were not protected where company notified employee that company emails are monitored). However, in-house counsel should be mindful that accessing work-related informa-

Byron McLain *is a litigation partner and member of the Government Enforcement Defense & Investigations Practice at Foley & Lardner LLP. He recently served in the Major Frauds Section at the U.S. Attorney's office in Los Angeles and as an assistant United States attorney from July 2012 to November 2018.*

FOLEY
FOLEY & LARDNER LLP

Hawwi W. Edao *is a litigation associate at Foley & Lardner LLP.*

tion on an employee's personal device without an employee's consent is more difficult. But it is not impossible. This business correspondence (particularly emails and text messages from private cellphones and computers) also can be accessed by the company in certain situations.

Recommendations to General Counsel at Regions Corporation

- Ensure the company's policies clearly, broadly, and expressly state that the company has the right to access data stored in company systems and devices, and the company reserves the right to access, monitor, intercept, or review any employee's company system and device usage if necessary. Make sure employees have signed a written acknowledgement of their receipt of, and agreement with, this company policy.
- Negotiate with the employee for the company to gain access specifically to any work-related emails or text messages located on the employee's personal devices and email accounts. This conversation with the employee should occur while the employee is still working for the company so the company maintains some leverage in these negotiations. However, the company should follow its own "Bring Your Own Device" workplace policies and consult outside counsel to ensure it is not accidentally violating any provisions of the Stored Communications Act.
- Lock the employee out of all company systems, retrieve all company property, and consider what status to place the employee on while you conduct an internal investigation (independent of any government investigation) in furtherance of a "legitimate work-related rationale."
- If company data has been compromised in the fraud, ensure the company complies with all applicable state data breach notification laws to inform its employees or clients of potential abuse concerning their personal information. However, the recommended actions an entity should take if it experiences a data security event, incident, or breach vary depending on the specific circumstances and the exact residency of the person or entity affected by the data breach. Since states are frequently changing their data breach statutes and notification requirements, always consult legal counsel for the most updated analysis concerning a specific incident of any data breach, particularly one involving COVID-19 relief fraud.
- Determine if any of the compromised data and information at the given company belongs to a different corporate entity. If a separate company's information is compromised due to the breach, there may be obligations under the contractual relationship between the businesses that should be addressed in addition to the state breach notification laws.

Question 2: What level of cooperation should the company provide with the federal investigation into the criminal allegations?

At the same time that Regions Corporation is conducting its internal investigation, the general counsel receives a phone call from the FBI. The FBI notifies the general counsel that Michael Henobetter had a company-issued laptop and a personal phone in his possession during his arrest. The FBI agent asks the general counsel for Region Corporation's voluntary consent to search the laptop. The general counsel, however, knows that the company's laptops contain proprietary and confidential intellectual property information belonging to the company. The FBI agent also indicates that he will issue Regions a subpoena with responses due in two weeks. The FBI agent has a laundry list of categories that he wants Regions Corporation to search within its company for discovery related to the COVID fraud scheme. After the general counsel hangs up with the FBI agent, she immediately contacts her outside corporate counsel, Brian Formerausa.

Brian is a past federal prosecutor and knows that FBI agents often request a much broader array of information than they are entitled to seek. Brian immediately calls the federal prosecutor assigned to the case and narrows the scope of the inquiry by finding out the particulars of the alleged COVID fraud relief scheme (i.e., the names of the co-schemers, the limited timeframe at issue, and the specific COVID program at issue). Brian also knows that Regions Corporation legally could provide to the government the expansive access it requested. For example, the 9th Circuit Court of Appeals' decision in *United States v. Ziegler* holds that an employee's "interest may be subject to the possibility of an employer's consent to a search of the premises which it owns." 474 F.3d 1184, 1191 (9th Cir. 2007) (company can give valid consent to a search of the contents of an employee's workplace computer even if the employee placed personal items in it). Nevertheless, Brian Formerausa requests that the government provide a subpoena and a search warrant limited in scope to probable cause, to protect the company's interests. Brian negotiates the scope of those requests with the FBI agent and the corresponding federal prosecutor.

Recommendations to General Counsel at Regions Corporation

- Keep the circle of information concerning the fraud investigation small. The company should subject as few employees and as little company information to the government's investigation as possible.
- Make a fair, measured, and reasonable interpretation of the government's subpoena language to identify and gather responsive documents. Outside counsel should assist with this process by directly communicating with the prosecutor on the scope of the subpoena, any possible ambiguities present in the language of the subpoena, and the deadline for producing information. Subpoena deadlines are often negotiable, but the government just wants an indication that the company takes the requests seriously.
- Confirm the list of searchable terms with the government through outside counsel. Document searches can be extremely expensive, so utilize outside counsel to narrow the search requests based on the exact information the investigating agents need.
- Request that the investigative agent obtain a search warrant to independently review any company property (i.e., a laptop). After the search warrant is obtained, ask for a copy of the search warrant to confirm that its scope does not intrude upon the company's confidential and proprietary information outside the scope of the alleged COVID-relief fraud.

Question 3: How should the company treat the accused employee's job status during the course of the investigation?

Immediately after the general counsel at Regions Corporation received notification that Michael Henobetter was arrested for alleged bank fraud for a PPP loan scheme, she placed him on paid administrative leave. She also received a phone call from Michael, where he swore that he had done nothing wrong and wanted to come back to work. The general counsel was very aware of the increased progressive climate at her company, and she did not want to overreact to the arrest. However, she also knew that Michael was an at-will employee and that she could terminate his employment even without cause. Ultimately, the general counsel knew that she had to do what was in the best interest of the company.

Recommendations to General Counsel at Regions Corporation

- Assess the company's policies and contracts with its employees for guidance on the situation, to determine if the employee is at-will or subject to an employment contract. Identify any contractual limitations to terminating the employee.
- Evaluate the egregiousness of the alleged PPP fraud and whether the company's decision concerning the employee's job status aligns with company culture. Review the company's own policies (e.g., Code of Conduct policy) to determine whether the alleged conduct is a violation of company policy (e.g., improper use of company property).
- Evaluate whether the company should keep the employee on paid or unpaid administrative leave during the pendency of the investigation or terminate him immediately.

In summary, government investigations, especially those related to alleged PPP fraud involving employees, can be unsettling for a company and specifically for in-house counsels who are often at the forefront of the company's response to the government. ■