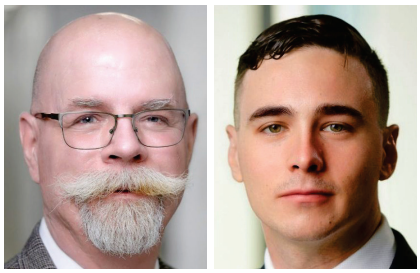
RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
VOLUME 35 NUMBER 11 ■ Part of the BRIDGETOWER MEDIA network ■ JUNE 11, 2020

Protecting against workplace fraud in the COVID-19 era



SPECIAL TO THE RBJ
John G. Schmidt Jr. and G. Michael Seaman

Over the past few months, there were many changes imposed on us all. Much of the economy was shut down, and then (at least in New York state), businesses either had to qualify as essential businesses and open back up (with precautions or limitations), or were forced to stay closed.

There is no dispute that these transitions are stressful and disruptive. Even if you are experiencing a heightened sense of community, or eagerness in the reopening process, all of this has created uncertainty. And as a rule, we are at our most vulnerable during periods of transition. Fraud is no exception to this rule.

Just as businesses strive to develop new strategies to survive the COVID-19 pandemic, so are "the bad guys." During the best of times, workplace fraud can strike anyone. During the pandemic, fraudsters have new opportunities to exploit this crisis for financial benefit.

At its core, workplace fraud takes a number of basic forms: check manipulation, cash skimming, bid rigging/kickbacks, over-ordering, credit card fraud, expense account padding, fake vendors, counterfeit materials, invoice or price manipulation, time fraud, outright theft, cyberattacks, conversion of confidential business information or trade secrets, and diversion of business opportunities.

The conditions that give rise to workplace fraud can also be categorized generally as:

The perpetrator with a motive — a disloyal, disgruntled or distressed employee, principal, executive, vendor, competitor or just a plain old outsider; with

Opportunity — some combination of reduced oversight and internal controls, scarcity of resources, lack of training on new procedures, lifestyle upheaval, new vendors, and/or new customers.

These conditions can all provide great opportunities for someone looking to exploit these vulnerabilities.

Now, add a pandemic and government shutdown to the equation. While the types, motives and opportunities of workplace fraud are fairly limited in number, their variations are endless. A bad actor — sometimes your most trusted employee — will attempt to cloak (or justify) his or her schemes in the circumstances of current events, with the COVID-19 pandemic being no exception.

As a result of COVID-19 and the related government shutdowns, many of the above opportunities for fraud have arisen. For instance, in New York state, Gov. Andrew Cuomo's Executive Orders mandated that many "non-essential" businesses reduce their on-site workforces to zero. This required a monumental shift to telework — a natural consequence of which is reduced oversight.

If you had an on-site workforce — be it 24 or 240 people — and were forced to scale back on-site personnel by up to 100%, how did that affect your internal controls and segregation of duties? Were you forced to sacrifice checks and balances regarding accounting, payroll, cash handling, collections, payables, vendors, procurement, and mail handling? How is confidential business information being handled in this new age of mass telecommuting? How is your cybersecurity?

Even at a basic level, is every telecommuter putting in an honest day's work for an honest day's pay? For some, telecommuting may lend itself to time record manipulation. Fortunately, while time fraud is simple, so are the countermeasures — the simplest being contact. Consider increasing the frequency of contact with employees to establish a baseline for productivity. Where frequent contact is difficult due to time zone differences or number of employees, employers may consider time tracking or monitoring software.

Telework also increases the risk of cyberattacks in virtually every form. Scammers adapt to prey on people's fears via malware under the guise of "tracking" COVID-19. Likewise, scammers disguise emails as if they

originate from legitimate health organizations, such as the Centers for Disease Control and Prevention, to conceal malware or phishing schemes. These schemes exploit users by taking advantage of their vulnerability — putting business networks at risk of data breaches, malware or ransomware. These issues can be costly. As businesses become increasingly reliant on telework, it is vital that they invest in appropriate IT solutions to counter these threats.

Businesses should also be aware of the potential for fraud posed by mandated reopening requirements. The new, pressing demand for personal protective equipment (PPE) and cleaning services lends itself to several types of classic business fraud—price gouging, false vendors, kickbacks and counterfeiting. Price gouging recently received a great deal of attention after a Brooklyn man was caught hoarding medical supplies, which he was selling at a 700% markup. Did you make a large upfront payment to a vendor who failed to show? Is it possible that the vendor does not exist anywhere except in the mind of a dishonest employee who converted the payment?

Counterfeiters are likewise able to thrive in a demand-heavy market for PPE and cleaning services. Businesses must be wary of whether the PPE they purchase and cleaning crews they hire are legitimate or are putting both their revenue and employees' health at risk.

While these schemes may be evolving, the preventative measures remain the same. The best way to prevent against purchasing counterfeit goods or paying false vendors is through research and due diligence. Recognize red flags: How long has the potential vendor been in business? Do they have any reviews? Do they have a brick-and-mortar establishment, or do they have only an online presence? Likewise, shopping around to determine a baseline for pricing before purchasing PPE can assist in protecting against price gouging.

If your business is the victim of workplace fraud, proactivity is key. Where there is smoke, there is probably fire. Initial discoveries usually involve just the tip of the iceberg.

When investigating fraud, proper evidence handling, security and confidentiality are important — for legal and strategic reasons. Working with counsel can provide some measure of confidentiality through the attorney-client privilege and attorney work product doctrine. Check your insurance policies, and make sure communications with the insurer are timely and accurate. Particularly during a crisis, your agent or insurer should not be the last word on whether you have coverage.

Investigation and legal strategy are very fact-specific. Should you pursue civil remedies or simply call the police? Do both? With experienced counsel, you can better determine the merits and scope of your situation. Are there witnesses? Who can be trusted, and who creates suspicion? Is evidence going to be mostly in the form of witness testimony, or electronic data — who or what might be a "smoking gun"? And how do you properly obtain and preserve that data or testimony? Consider who will handle employee, customer and public relations. Does your industry or profession have self-reporting or other regulatory requirements?

If you go the civil litigation route, do you need emergency or preliminary relief to stop the bleeding — to maintain the status quo, preserve stolen assets or intellectual property, or prevent business diversion or unfair competition? Do you need to regain immediate possession of converted property or data, or at least stop the thief from using or destroying it? Review operative agreements — be it with a shareholder, employee or vendor. Does it articulate or limit remedies, provide for attorneys' fees to the party seeking to enforce the agreement, or require the target to insure you?

The bottom line — we have had a historically difficult year so far. Taking the necessary steps now to ensure that you protect your business as we move forward may be the difference when faced with the potential threat of workplace fraud. Should your business come across a developing issue, proactively seeking assistance will not only mitigate your harm, but better position you to overcome these uncharted waters.

John G. Schmidt Jr. is a partner with Phillips Lytle LLP and co-leader of the firm's Commercial Litigation Practice Team. He concentrates his practice in the areas of business disputes, commercial litigation, employee disloyalty, technology litigation, computer forensics, white collar/government investigations defense, and class action defense. He can be reached at (716) 847-7095 or jschmidt@phillipslytle.com.

G. Michael Seaman is an attorney with Phillips Lytle LLP, where he concentrates his practice in the areas of commercial litigation, data security and privacy, and white collar criminal defense and government investigations. He can be reached at (716) 847-5437 or gmseaman@phillipslytle.com.