COVID-19: Detecting Fraudulent Schemes Perpetrated by Employees

Jim Patterson and Amanda McLachlan

Recent media coverage has focused on the effect of COVID-19 on the emergence of cyber related frauds, including social engineering and phishing schemes. Employers would also be wise to consider the unique opportunities for fraud detection arising from government-mandated shutdowns, social distancing and the prevalence of employees working remotely. The recent work from home phenomenon may enhance the effectiveness of internal controls designed to detect any previously well-tended fraudulent employee schemes, including secret commission or kickback schemes, procurement and supply chain fraud, inventory theft, phony invoicing and other dishonest or fraudulent schemes.

A common internal control designed to detect employee fraud is the implementation of mandatory vacation policies. Proper division of duties (for example, separation of purchasing and payment functions) and the regular rotation of employee job functions are also important internal controls. Such controls are intended to reduce the risk arising from one employee maintaining sole control over key business or accounting functions in furtherance of a fraudulent scheme. Many employee frauds are only discovered following the implementation of such controls or changes to existing procedures brought about by operational changes. When an employee is away from his or her normal operational duties this can provide an opportunity for superiors, co-workers and internal auditors to detect the previously well-guarded secret fraudulent scheme. The current remote work environment necessitates operational change and the potential for enhanced division of duties. This creates an opportunity for employers to detect a dishonest employee's ongoing fraudulent scheme.

Kickback or Secret Commission Schemes

Kickback or secret commission schemes are common forms of employee fraud. Kickback schemes often follow a straightforward recipe: a supplier offers money or some other incentive to an employee to induce his or her employer to purchase a service or product at an inflated price. A supply chain fraud typically involves the insertion of an intermediary into the supply chain, with the employer paying an inflated price to the intermediary to the benefit of the dishonest employee. Kickback and supply chain schemes can be difficult to detect in the absence of robust tendering and procurement controls, routine job duty rotation, division of duties and mandatory vacation policies.

Canadian criminal law prohibits secret commission schemes. Section 426 of the Criminal Code prohibits the payment of secret commissions to an agent, as well as the receipt of secret commissions by an agent. Similarly, at common law, both the party paying the secret commission and the party receiving the secret commission are liable for losses arising from the scheme.

Red Flags of Employee Fraud

- Sole Source of Supply – Some frauds involve employees dealing directly with customers or suppliers to carry out the scheme. This may prove impossible if that employee is absent from work or self-isolating due to COVID-19 restrictions. Employers should be mindful of sole source of supply in the face of other commercially viable options.

- Control of Procedures – Employees who are stealing from their employers often engage in a pattern of conduct designed to circumvent internal controls. An employee who is unusually possessive of internal controls and procedures may also warrant closer scrutiny. This is particularly true where that employee takes a sudden interest in operations beyond the scope of his or her own job duties. Close relationships with employees in departments with access to accounting or procurement procedures may warrant further investigation. An employee required to work remotely due to COVID-19 may lose the ability to control such procedures.

- Perfect Attendance – An employee's refusal to take a sick day or vacation could signal an attempt to conceal a fraud. Employees perpetrating a fraudulent scheme may insist on attending work daily to maintain their ability to bypass existing internal controls to ensure that evidence of their wrongdoing remains concealed. Current COVID-19 restrictions in place requiring certain employees to work from home may impede the ability of employees to continue such schemes undetected.

A Time for Increased Vigilance

While the temptation in trying economic times may be to shift focus to pressing operational and other organizational needs, employers should maintain robust internal controls while employees are working remotely due to COVID-19. Employers should also consider whether additional or modified internal controls are required to combat the challenges of the current working environment.

With many employees working remotely, employees perpetrating fraudulent schemes may no longer be well positioned to intercept correspondence, control office procedures and daily interactions or accounting/ procurement activity in order to conceal the scheme.

Discovery of a Fraudulent Employee Scheme

Upon discovery of a fraudulent scheme perpetrated by an employee it is imperative that employers act quickly to properly investigate with the assistance of experienced legal counsel. Effective legal risk management will require the consideration of several legal issues, including financial, regulatory and reputational risks, employment law issues, fidelity insurance coverage and other potential avenues of recovery of financial losses.

Jim Patterson
Partner
416.777.6250
pattersonj@bennettjones.com

Amanda C. McLachlan
Partner
416.777.5393
mclachlana@bennettjones.com