COVID-19 Fraud Risks: Remote Working, Internal Controls and Corporate Disbursement Fraud

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

COVID-19 Fraud Risks: Remote Working, Internal Controls and Corporate Disbursement Fraud

What impact has COVID-19 had on increased fraud risk and exposure to additional threat actors as it relates to corporate disbursements?

That is the question we often receive from our clients as we continue to navigate the unfamiliar waters of a global pandemic and maintain consistent and effective business operations with a remote workforce. More importantly, we are now confronted by additional fraud risks given required changes in how a company's control environment can remain appropriately designed and operating effectively with employees completing most of their day-to-day work outside of the office.

We are all familiar with the three key aspects, common in increasing the risk of fraud: 1) Opportunity, 2) Attitude and Rationalization and 3) Incentive and Pressure. With employees working, almost exclusively, from home, COVID-19 has provided the perfect **OPPORTUNITY** for threat actors to breach the security of companies with informal or unstructured control environments. More specifically, a common area for fraud and loss is within the process of corporate disbursements and ACH payments. Employees responsible for processing vendor bank account changes, address changes, corporate disbursements and other duties within the payables function are now faced with performing these tasks in unfamiliar or abnormal work environments. For companies without a focused effort on internal controls, this can increase the risk of error and the opportunity for threat actors to commit fraud.

As outlined in the 2020 Phishing and Fraud report published by F5 Labs, "Phishing remains a popular method of stealing credentials, committing fraud, and distributing malware. But what appears on the surface to be a juvenile form of cybercrime can be, in practice, a well-orchestrated, multi-faceted, and sustained attack campaign by organized crime groups."[1] Although preventative cybersecurity controls provide the first line of defense against phishing attacks and other forms of cybersecurity threats, companies can further protect themselves from disbursement and ACH payment fraud by ensuring the internal control environment is standardized, managed and monitored at the appropriate levels.

Asking the following questions can be the first step in identifying potential gaps within the corporate control environment:

- How are job duties segregated among accounting personnel?
- Do inconsistencies exist within our processes and control ownership?
- Are employees appropriately trained?
- Do fraud risk monitoring activities exist?
- Does management oversight exist to sufficiently monitor potential control failures?

In addition to bringing attention to the increase in phishing schemes, the Association of Certified Fraud Examiners (ACFE) has published the "Top 5 Fraud Schemes: Predicted Increase Over 12 Months, Due to Coronavirus."[2]

As evidenced in this data, the need has never been greater for integrated and mature risk mitigation protocols.

The current and projected increase in payment fraud of 85% through 2020 has had a direct impact on corporate financial stability. Significant losses derived from payment fraud, due to lack of adequate corporate controls, can be the difference in weathering the storm through a global pandemic and economic crisis.

More specifically, mitigating corporate disbursement and ACH payment risk can begin with answering the following:

» Who has authority to make changes to vendor payment information and address?
» Do policies and procedures exist to govern changes to the vendor master file?
» How are changes to payment information monitored and approved?
» Do controls exist to segregate roles and responsibilities within the disbursement process?

The following best-practice controls should be considered to assist in mitigating the risk of corporate disbursement and ACH payment fraud:

IT & Cybersecurity	» Cybersecurity and corporate IT policies » Cybersecurity awareness training » Real-time phishing and malware incident monitoring and report review	
Vendor Management	» Vendor management and change policies » Vendor change approval and call-back controls » Vendor ACH and address change monitoring and report review » Management oversight and monitoring on the design and effectiveness of control execution	
Payment Processing	» Delegation of authority matrix on payment approval » Check register and vendor ACH disbursement review » Dual approval and dual signature disbursement requirements	
External Vendors	**Preventative Controls**	**Detective Controls**
	» Sophisticated malware solutions » Third-party banking, vendor payment information verification services » Third-party banking, positive pay services » Business process reviews and risk/control assessments	» Data Forensics Indicident Report (DFIR) » Third-party penetration testing

Developing awareness and understanding of these new fraud risks is the first step in mitigating the risk of payment fraud. However, focusing on a culture of strong internal control is imperative to ensuring the lasting health and growth of any organization.

Schneider Downs offers several risk advisory services to help our clients navigate these changing business risks. As part of these services, we work with our clients to assess control environment maturity and develop appropriate risk mitigation plans to enhance corporate governance and control activities.

Sources:
1 www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report
2 ACFE: Fraud in the Wake of COVID-19: Benchmarking Report (www.acfe.com/covidreport.aspx)

Contact Us

To learn more about our cybersecurity and IT risk advisory services, please visit www.schneiderdowns.com/cybersecurity or contact us at cybersecurity@schneiderdowns.com.

For more information on Business Process and Financial Risk Advisory services please visit our website at www.schneiderdowns.com/risk-advisory-services or contact James B. Yard at jyard@schneiderdowns.com.