

# HR NEWS



## HR Lessons Learned During the Pandemic

---







# Combating COVID-19-Related Fraud Starts With Training Employees

By Kenneth C. Pickering

**H**uman resources professionals have had an increasing array of issues to manage during the COVID-19 pandemic. As we move into the new normal of vaccine availability, HR professionals must focus increasingly on COVID-related fraud.

Cybercriminals have stepped up attacks on organizations of all types, frequently targeting employees with phishing and identity theft attempts as ways to circumvent cybersecurity measures such as firewalls and data encryption. The trend has caused employers to both invest in enterprise-wide cybersecurity resources and equip employees with best practices. As a result, HR professionals should put extra emphasis on employee cybersecurity training.

## How COVID-19 Increased Risks

Researchers have long known that natural disasters and times of economic upheaval give rise to the types of uncertainty and anxiety that make people more susceptible to the emotional and physiological pleas of fraudsters. The onset of the COVID-19 pandemic in the United States in March 2020 had much the same effect, bringing with it significant social, economic and physiological stresses.

Overnight, individuals' support networks and routines were drastically altered. People found themselves cut off from familiar social interactions and their normal ways of doing business in both their professional and personal lives.

For those whose jobs permitted it, transitioning to working from home meant utilizing internet services and online vendors. Everyone in general became more active online, regardless of their work situation. As a result, the transformation into an online information economy that was already underway accelerated.

Economic and societal shifts led to a reduction in face-to-face interactions, and the increase in internet usage invited an attendant surge in online criminal activity. Since the 1990s, greater internet use has been a consistent predictor of increased fraudulent activity.

Recently, more people than ever before have been the targets of fraud while working and shopping from home. At the same time, individuals' heightened levels of fear and anxiety make them more likely to fall prey to COVID-related fraudsters offering everything from fake treatments to assistance with contact tracing efforts or economic relief.

Uncertainty and misinformation about the pandemic created a nearly perfect online environment for criminals looking to exploit changes in social and economic interactions. Fraudsters and cybercriminals seized on opportunities to exploit systems' vulnerabilities and take advantage of individuals by heightening angst and using manipulative appeals. A fraudster's goal might be convincing someone to buy fraudulent products or services or to disclose personal or business information.

## COVID-Related Fraud Takes Many Forms

Again, fraud and cybercrime have been on the rise throughout the pandemic. The Federal Trade Commission detected more than twice as many cases of identity theft during 2020 than in 2019. The National Credit Union Administration warned members in August 2020 of spikes in new account fraud, identity theft, money mule schemes and cybersecurity risks associated with mobile banking apps as fraudsters exploited vulnerabilities in institutions' remote access systems.



In its December 2020 benchmarking report titled *Fraud in the Wake of COVID-19*, the Association of Certified Fraud Examiners revealed that 79 percent of the organizations responding to its most recent survey experienced an overall increase in fraud. Incidents included cyberattacks on computer systems and employee-related fraud such as embezzlement and other forms of defalcation. As a result, nearly half of the survey respondents planned to increase their organization's antifraud efforts by doing things such as enhancing investments in antifraud technology and bolstering antifraud staff.

Clearly, pandemic-related fraud takes many forms and encompasses a wide range of scams targeting both organizations and individuals. A common tactic involves exploiting uncertainty and anxiety over COVID-19 to seek payments for fake products and services purported to treat or ward off infections. Scam contact tracing calls and fake offers of financial relief from the government are also commonly used in attempts to gain access to personal and business information.

Now, as if nearly two years of living through a pandemic has not been worrisome enough, supply chain issues and financial challenges such as inflation have made the economic outlook for many people uncertain. One of the three prongs of the fraud triangle—perceived need—has been exacerbated as a result of the economic uncertainty brought to bear by COVID-19. Employees' own feelings of insecurity create circumstances favorable to theft from employers via embezzlement, vendor fraud, skimming and bank fraud.

## Vaccine Fraud Is an Emerging Concern

Sales and use of fraudulent vaccination cards have spiked as more employers require employees to either provide proof of having been vaccinated or undergo regular COVID-19 testing. Check Point Research estimated that from August to September 2021, the number of internet sites offering forged vaccination cards and test results rose tenfold from 1,000 to 10,000. This increase coincided with the rollout of employer mandates and requirements to prove vaccination status to enter various venues. It also highlights fraudsters' adaptability as the pandemic itself evolves.

In some instances, the fraudsters turn out to be medical professionals. The U.S. Department of Justice reported on July 14, 2021, that it had arrested a California-licensed naturopathic doctor for allegedly selling fake vaccination cards and "immunization pellets," which she claimed would provide lifelong immunity against COVID-19.

It is interesting to note that individuals would take an untested immunization pellet and obtain a fake vaccination card instead of getting an FDA-approved vaccine. Misinformation and distrust of traditional governmental oversight and regulatory agencies play

into the hands of fraudsters looking to take advantage during times of economic or social crises.

## Recommendations for HR Professionals

As more employees started working remotely, the number of individuals targeted by phishing emails and other attempts to access and compromise employers' computer systems rose. This reinforced employees' role as frontline defenders against COVID-related cyberattacks.


Increasing employees' knowledge of cyber threats to themselves and the organization is key to combating fraud. The greatest risk is business email, which cybercriminal use to introduce ransomware and malware, as well as to obtain passwords. Once a cybercriminal has the necessary access to computer systems, they can steal data and perform hacks.

Especially when employees work remotely, employers should rely on multifactor authentication for logging in to email and other apps. When feasible, employers should also consider integrating biometric security features such as fingerprint readers. Looking beyond employees themselves, AI monitoring can flag potentially fraudulent activity such as suspicious login patterns, malicious emails and unusual customer activity.

Above all else, employees should be urged to double-check web address details before clicking links in emails, to never download attachments from unknown sources, and to not provide personal or financial information to untrusted websites. Sharing information with individuals who make unsolicited phone calls should also be strongly discouraged.

As is often said, an organization's greatest resource is its people. When it comes to fraud, an organization's greatest threat is likely to also be its people. Keeping employees up to date and informed about cybersecurity issues and risks to their personal health and finances by providing ongoing training will help them help the organization combat COVID-related fraud. Ensuring employees have trustworthy information can also reduce the stress and anxiety they may be experiencing.

---

*Kenneth C. Pickering is a partner in the law firm of **Mirick O'Connell** in Worcester, Mass. As a member of the firm's Business Litigation Group and head of Mirick O'Connell's Government Investigations Team, Pickering has conducted numerous fraud investigations on behalf of employers and individuals. —*