The Work Week

Bassford Remele Employment Practice Group

February 23, 2026

Welcome to another edition of *The Work Week with Bassford Remele.* Each Monday, we will publish and send a new article to your inbox to hopefully assist you in jumpstarting your work week.

Bassford Remele Labor & Employment Practice Group

Who You Gonna Call?
How Employers and HR Professionals Can Avoid and Deal with So-Called "Ghost Employees"

Andrew T. James and Rachel A. Ball

A six-figure salary, annual bonuses, and a four-year tenure—all for an employee who never sent a single email or logged into a project. The recent guilty verdict in the Optum "ghost employee" case is a stark warning that remote work environments, if not properly audited, are ripe for sophisticated internal fraud. Whether you have a $1 million phantom in your payroll or are just a conscientious employer looking to avoid being taken advantage of, some simple proactive steps will help protect your business.

Overview and Facts of the Optum Ghost Employee Case

A "ghost employee" is an individual on a company's payroll who does not perform any legitimate job duties. The term can be a misnomer; ghost employees are often real people, including former employees left active or individuals whose identities are misused to route payments.

As the recent guilty verdict of Karan Gupta in the *Optum* fraud case underscores, this practice constitutes fraud and misuse of payroll funds, exposes employers to regulatory and criminal scrutiny, and signals material weaknesses in internal controls. The facts of the case should concern any employer with remote employees.

This past week, on February 17, 2026, a Minnesota jury found Gupta, a former Optum senior vice president for data analytics based in California, guilty of defrauding his employer by hiring a friend for a full-time remote position—an IT data analytics manager—supervised by Gupta. To

secure him the position, Gupta helped his friend, Shangraf Kaul, prepare a resumé that misrepresented Kaul's qualifications. According to publicly reported allegations and findings, Kaul performed little or no actual work for almost four years, all while collecting a salary that started in the six-figures, plus annual raises and bonuses. Gupta collected more than half of the unearned salary in kickbacks. Optum discovered the fraud after Gupta was terminated in November 2019 for a separate incident.

When the manager replacing Gupta reached out to Gupta's direct reports, Kaul did not initially respond but subsequently indicated he had been out of the country dealing with an ill family member and then gave notice of his immediate resignation from Optum. When the manager inquired about Kaul to Gupta's remaining direct reports, no one knew him or knew what he was working on. Optum then reviewed Kaul's laptop, which contained no work product at all, and his email account revealed nothing to indicate he was working on any projects. Kaul never sent an email or accepted a group calendar invite, and his calendar showed only one meeting: a recurring weekly meeting with Gupta. When Optum received Kaul's laptop following his resignation, they found the screen severely damaged, the battery not in working order, and no power cord.

According to filings in the criminal case, Optum's system locks a person's credentials if they do not login for 17 days straight. From 2016 to 2019, Kaul's credentials reflected frequent 17-days stretches where he did not login to his computer, and the company needed to unlock his login.

After its investigation, Optum referred the matter to law enforcement. Gupta was charged in a 12-count federal criminal indictment, including one count of conspiracy to commit wire fraud, ten counts of wire fraud, and one count of conspiracy to commit money laundering. Kaul pled guilty and served as the star witness for the Government at trial. After a five-day trial, on February 17, a Minnesota jury found Gupta guilty on all 12 counts.

Legal Framework and Risk

As Gupta and Kaul now know, individuals who orchestrate or knowingly ignore schemes may face criminal charges, fines, and imprisonment. But employers, too, risk civil or criminal liability in ghost employee fraud schemes, including for restitution, disgorgement, civil penalties, debarment from government programs, and/or contract termination. Ghost employee fraud creates exposure across multiple legal domains:

- Wage and hour laws: Paying non-employees can taint recordkeeping, distort overtime calculations, and misallocate costs in a way that triggers audits and penalties.

- Payroll tax requirements: False payroll entries can constitute false returns, improper deductions, and failures to deposit or report, with associated penalties and potential criminal exposure.

- Internal fraud and theft statutes: Creating or maintaining ghost employees to siphon funds implicates embezzlement, wire fraud, bank fraud, and related offenses. Corporate

victims face loss recovery and insurance considerations; individuals who facilitate schemes may face criminal prosecution.

- False Claims Act implications: If payroll costs are charged to government contracts, grants, or reimbursement programs, paying ghost employees can constitute the presentment of false claims and false statements, invite treble damages and penalties, and expose both the organization and individuals to liability.

- Benefit plan and ERISA risks: Enrolling or reporting ghost employees can distort eligibility, contributions, and fiduciary reporting, potentially triggering fiduciary breach claims and corrective action obligations.

- Corporate governance and securities considerations: Material weaknesses in internal controls over financial reporting tied to payroll can trigger disclosure duties, restatements, and enforcement interest for public companies.

An employer could be held vicariously liable if the fraud was committed within the scope of the employee's employment, such as hiring and managing the ghost employee. Furthermore, the potential penalties are substantial. An employer's failure to implement reasonable controls to mitigate this risk can result in aggravated penalties, remedial obligations, or even punitive damages.

Red Flags and Prevention Strategies

Ghost employee fraud is most often perpetuated in employment settings with decentralized hiring, multi-entity structures, rapid growth, and outsourced or lightly supervised payroll operations. Basic controls must be both intentionally structured and rigorously enforced. Understanding how these schemes arise—and the red flags that accompany them—is essential to reducing exposure and potential liability.

One of the clearest warning signs is a breakdown in segregation of duties. As in the case with Gupta, when a single employee has authority to add new hires, approve time entries, and review a subordinate's work, the opportunity for manipulation increases significantly. This risk increases exponentially if that same manager can process payroll changes, as well.

Employers should be alert to payroll records that lack complete personnel files, missing tax documentation, or identical bank account details shared by multiple employees. Regular reconciliation of payroll registers to active headcount reports, combined with independent review of new-hire documentation, can reveal inconsistencies before losses compound.

Data analytics can also be a powerful detection tool. Unusual patterns—such as payments issued outside standard payroll cycles, employees without benefit deductions, or multiple employees sharing mailing addresses—should trigger review. Periodic internal audits, surprise headcount verifications, and direct deposit audits can uncover anomalies.

Employers with remote or multi-site workforces should consider requiring supervisory confirmation of active employment status at regular intervals, particularly before year-end reporting. And, for those employers whose system locks an employee out after a set period of time without logging in, any lock-outs should prompt a thorough review of the employee's productivity and usage of the employer's IT infrastructure, such as email, centralized servers, and networks before granting the employee access again. Given the importance of offering remote work for both retention and recruitment, it is vital for employers with remote employees to have a clear written policy setting forth objective, verifiable performance expectations, and to regularly audit those policies and ensure employees are meeting those expectations.

Employers should ensure hiring decisions are made by a team, a candidate's resumé is verified and professional references are checked, and that several layers of supervisory staff meet with remote employees on at least a semi-regular basis. Subject to state and federal laws regarding employee monitoring, employers should consider utilizing authenticated timekeeping with geolocation, as well as flagging zero-activity periods for salaried roles. For those companies with staffing agencies and contingent labor, employers can reduce risk by requiring verified rosters, badging, time approvals by on-site managers, and periodic reconciliations to invoices and statements of work.

Finally, robust critical safety and security initiatives designed to encourage employees to report suspicious activity can be instrumental in unearthing fraud. Employers should ensure whistleblower channels are well publicized and that employees feel both safe and protected when reporting suspicious activity.

When Fraud Happens: Response and Remediation

When ghost employee fraud is suspected, an employer should immediately consult with a lawyer both to protect the company and ensure any investigation and evidence are appropriately preserved, consistent with chain-of-custody protocols to support potential civil recovery or criminal proceedings. Response and remediation require a swift pivot from investigation to enforcement: preserving the data trail; terminating the fraud loop; and coordinating with legal experts to manage the complex web of reporting obligations to insurers, boards, shareholders, and/or government agencies.

Conclusion

Ghost employee schemes are preventable with a culture of accountability supported by internal controls. Written payroll and remote work policies, periodic risk assessments and audits, and board-level oversight—particularly for larger or regulated entities—demonstrate diligence and reduce the likelihood that a fraudulent scheme will go undetected. By combining procedural safeguards with ongoing monitoring, employers can materially reduce the risk of ghost employee fraud and strengthen overall governance.

Bassford Remele's Employment group is experienced in working with local, state, and federal law enforcement on potential criminal matters arising within the employment context and here to

support employers facing such criminal misconduct in the workplace. We are available to help with reviewing your company's fraud-prevention controls and ensuring payroll and remote work policies mitigate risk while balancing the increasing need for a remote workforce. Please reach out with any questions or if you need assistance.

LEARN MORE ABOUT OUR EMPLOYMENT PRACTICE »»
