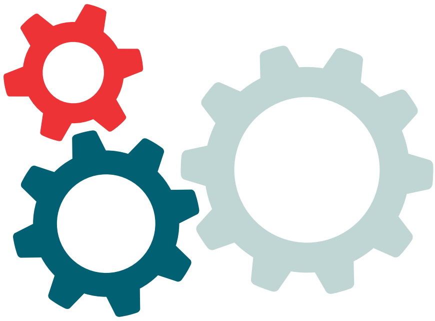
Preventing Common Types of Payroll Fraud

BY TONYA KEMP, CPP



Running payroll is a risky business, but when a company lacks the appropriate internal controls to manage its payroll, payroll fraud is often the result. An employee commits payroll fraud when they embezzle funds from the business by using the organization's payroll systems and processes.

There are numerous ways for someone to commit payroll fraud, but there are two types that are among the most common.

Fortunately, there are several methods your organization can use to detect these types of payroll fraud and prevent it from happening.

Two Common Types of Payroll Fraud

There are many different types of payroll fraud, but the two most common ones payroll departments run across are timesheet fraud and ghost employees. Let's look at each of these a little closer:

1. **Timesheet fraud**—Timesheet fraud happens when an employee claims to have logged more hours and is paid for hours never actually worked. This type of fraud happens more often than any other type of payroll fraud, especially when there are no controls or reviews in place to help detect it.

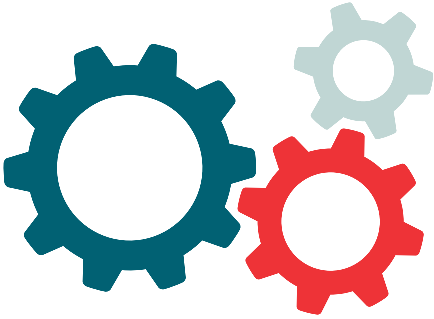
   One of the most common type of timesheet fraud is buddy punching. Buddy punching happens when an employee has a friend or another employee clock them in or out when they are not working or in the workplace. For example, "Sammy" clocks out for lunch at 1:00 p.m. and is taking a longer than usual one-hour lunch. He calls "Billy" and asks Billy to clock him back in at 2:00 p.m. Billy clocks Sammy in, and therefore has increased Sammy's worked hours, which will increase his pay, without him actually being at work. Proper time clock management can be especially difficult if you have a workforce that is scattered across multiple locations or states.

   Implementing an electronic timekeeping system that allows for biometric punching and geofencing is one technological solution that can help mitigate this type of fraud. Biometric punching is when an employee must clock in and out using biometrics such as facial or fingerprint recognition. The use of physiological traits to verify identity has greatly expanded and improved in recent years and most electronic timekeeping systems currently available can do this heavy lifting for you, thus reducing the temptation for employees to ask fellow employees to illegally punch them in or out. Having a zero-tolerance buddy punch policy, coupled with biometric punching capability, can help to reduce the risk of timesheet fraud. Make sure the policy is well-written and effectively communicated to staff members. Be sure to involve your HR, operations, and legal teams when drafting this policy. Enforce it by always following up on and dealing with all instances as soon they occur. It is also imperative that your organization establishes and communicates clear disciplinary actions that will be taken if anyone is caught violating this policy.

   Geofencing is another option used to deter buddy punching. Geofencing is when an electronic "barrier" is set up around the location in which an employee can clock in or out via a mobile app. It relies on GPS, WiFi, and cellular data to create a barrier around your business. Employers can decide how close employees need to be to clock in, whether it's the parking lot or the front door. This helps employees from being clocked in when physically still away from work or from being clocked in by someone else, thus eliminating budding punching.

2. **Ghost employees**—Ghost payroll is another common type of payroll fraud that occurs when someone makes up, or creates, a fictitious or "ghost" employee and adds them to the HR/payroll system and collects the wages. Ghost employees can also be non-active employees who have left the company but have yet to be removed in the system, allowing someone to use their active profile to add hours and make fraudulent payments. A field manager or someone who has access to enter a new hire, or enter and approve an employee's time, can commit such acts of fraud. When the fraudster leaves a salaried person active in the system, they are usually on a forecasted pay schedule. This means that they are automatically paid a certain number of hours or a set salary each payroll. In these cases, the fraudsters will reroute the employees direct deposit account and funds will continue to be paid until someone terminates the employee's record in the payroll system.

Tonya Kemp, CPP, is Director of Payroll Operations at Rent-a-Center, Inc. She is a member of the APA's Board of Contributing Writers for PAYTECH.



Payroll professionals can help reduce this type of fraud by creating controls, such as separation of duties to ensure that no one person is performing all the steps in the employee's life cycle. For example, the onboarding process should be handled by someone outside of payroll. If a person handles onboarding, they shouldn't have access to pay employees. However, read-only access should be considered. You must also ensure that the off-boarding process is performed in a timely manner. This is a control that should be tested frequently because it happens more often, and fraudsters are aware that they can gain access to more funds through salaried ghost employees. Therefore, payroll/HR should consider the following tasks/titles to ensure separation of duties to prevent this type of payroll fraud:

1. **Onboarding**—Recruiter or field manager
2. **Paycheck Preparation**—Payroll administration
3. **Paycheck Authorization (sign-off)**—Payroll manager or director
4. **Paycheck Distribution**—Third-party or payroll clerk
5. **Off-boarding**—HR administration
6. **Reconciliations**—Accounting team member or someone who didn't onboard the employee, prepare, or authorize payroll. Reconcile payroll accounts at least quarterly. The best practice to follow is to reconcile monthly to detect any possible fraud in a timely manner.

Another way to reduce the risk of ghost payroll employees is to create a process to review and audit your payroll. Some common audits that many payroll teams have put in place to detect fraud include bank account changes and address changes. When someone commits ghost payroll fraud, they will re-route the ghost employees bank account to their own account. This allows the fraudster to receive two direct deposits each payroll. In some cases, the fraudster and ghost employee may also share the same address.

Auditing social security numbers (SSNs) against names is another preventive measure you may want to implement to help catch ghost employees. For example, if your company doesn't use E-Verify or verify SSNs, a fraudster may create a separate employee profile or profile with another SSN that may be similar to another employee. Sometimes the SSN is only one digit off, the name and the date of birth may even be the same, but all other information is different. Best practice calls for the verification of SSNs with the Social Security Administration when an employee is hired.

These are just a few things your organization should review to help detect fraud associated with ghost payroll and to better protect your company assets. Furthermore, be sure to review and test your controls frequently to guarantee that they are working as they should and verify that no one has been ghosted.

Conclusion

Controls can either be policies, procedures, or technical safeguards that are implemented to protect an organization's assets. They can reduce the risk of payroll fraud such as timesheet fraud and ghost employees. Controls also hold team members accountable to monitor their company's assets. Remember, however, that not having them in place, whether you're a public or a private company, can increase the risk of fraud and be very costly to your company. Be proactive and detect these frauds early. ■