



## Paycor Security Frequently Asked Questions

### Q: Does Paycor have an independent audit of its financial statements?

A: Yes, Paycor financial statements have been audited annually since 1993, always with an unqualified opinion.

### Q: Does Paycor have a SOC1 audit?

(Also referred to as an SSAE 16 audit. Formerly known as a SAS 70audit)

A: Yes, Paycor engages a national public accounting firm to perform a SOC1 audit on an annual basis. The auditor's report describes and tests controls related to Paycor's payroll processing services for the period December 1st –November 30th. The current year's report is generally issued in early January of the following year.

### Q: Does Paycor segregate funds it holds for clients from its operating funds?

A: Yes, Paycor completely segregates funds held for clients from the Company's operating funds.

### Q: How does Paycor invest client funds?

A: Funds held for clients are invested according to a Board of Directors-approved investment policy. The objectives of that policy in order of importance are credit quality, liquidity and return. Paycor is also monitored by an audit committee composed of members from its Board of Directors.

### Q: Are funds held for clients reconciled on a daily basis?

A: Yes, Paycor performs daily reconciliations of all funds held for clients.

### Q: What other controls does Paycor have in place?

A: Paycor maintains the following separate departments to ensure proper controls and "segregation of duties":

- A separate tax department managed by operations for filing client payroll taxes.
- An ACH department in charge of electronic fund transfers.
- A credit department to monitor and reduce Paycor's ACH and other financial and operating risk.
- An independent accounting department with personnel whose sole responsibility is daily, monthly and quarterly reconciliation of all client fund accounts.
- A corporate treasurer and risk manager who oversees continuous enhancement and compliance with financial controls.

In addition, Paycor maintains the following controls:

- No access to check printing facilities by personnel who process payroll or interact with clients.
- An information security program in compliance with the Gramm-Leach-Bliley Act to protect confidential customer information and to respond to incidents in a timely manner.
- Regular IT system audits by external third party security experts.
- Secure access to all processing facilities.
- Locked shred bins throughout its processing facilities.
- Multiple firewalls, antivirus/malware protection, web filtering and other multi-layered security technologies.

### Q: Does Paycor have protection against employee theft and fraud?

A: Yes, Paycor carries commercial crime insurance of \$10,000,000 to cover Paycor employee theft of client funds and an Errors and Omissions policy of \$3,000,000 per occurrence with a \$3,000,000 aggregate.

### Q: Does Paycor have a disaster recovery/business continuity plan in place?

A: Yes, Paycor has a disaster recovery and business continuity plan, both of which are reviewed and tested throughout the year. Paycor's data is replicated to an offsite hosted facility in near real-time, and Paycor maintains redundant processing centers in three cities. Data is also backed up to tape nightly. Paycor's Data center and headquarters are protected by two diesel powered generators that automatically turn on in the event of a power failure.