CPA
Practice Advisor

bad actor washed a legitimate check and cashed it. Cases of check theft dipped in the early 2010s as companies and banks shored up their security.

Jan. 15, 2020

Most companies have experienced at least one instance of check theft, in which a bad actor washed a legitimate check and cashed it. Cases of check theft dipped in the early 2010s as companies and banks shored up their security. But according to the Association for Financial Professionals' "Payments Fraud and Control Survey Report", 82% of companies experienced fraud in 2018—the highest number in a ten-year period. The fraud was a blend of old-school check and new electronic payment security threats. This is because as companies adopt more processes for each payment type they utilize, another set of potential security threats also emerges.

Electronic payment fraud occurs most commonly when AP teams make changes to secure data—which, in this case, refers to data such as bank account information, remittance email addresses, and recipient names. Criminals hack into company

Any company that you share sensitive data with should be protected by the highest industry security standard. The following list is a variety of compliance types and security procedures which potential providers may mention:

1. SSAE 16 and SOC Compliance

SSAE 16 replaced SAS 70 as the definitive security guide in 2010. SSAE 16 compliance includes SOC auditing, which publicly tracks company compliance statuses. Three types of SOC auditing exist:

- SOC 1: Heavily audits internal controls of a service organization. This report can be used by an entity to assess a service organization for relevant and effective controls. Typical entities include, but are not limited to, publicly traded companies subject to SOX reporting (see below).
- SOC 2: Heavily audits data relating to the Trust Services Principles (TSPs) in information security: Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- SOC 3: Lightly audits IT controls relating to TSPs. This audit’s controls are more relaxed than SOC 1 and 2.

2. SOX Compliance

Also known as Sarbox compliance (in reference to the Sarbanes-Oxley Act created in the early 2000s), SOX compliance is a set of government-mandated regulations to which publicly traded companies must adhere. These regulations offer transparency into companies’ financial records, as well as their wholly-owned subsidiaries. It was enacted to protect shareholders from dishonest internal practices. If your provider is either a publicly traded company or the wholly-owned subsidiary of one, they are legally required to be SOX compliant.

3. PCI DSS Compliance

PCI DSS compliance—or “PCI compliance” for short—audits companies associated

other ways than the guarantee—for example, you may be covered for forgery or other fraud instances. Before signing on with a provider, take a moment to ask them if you are also covered under their insurance plan, and for what instances.

5. Employee Security Training

Because fraud often occurs due to human error, staff security training is key to prevention. Ask your provider what sort of training their employees undergo—especially those who interface directly with your vendors. Many providers also have other protocols in place, such as using security questions to verify calls. Understand the measures your provider takes to protect your company’s financial wellbeing.

6. Positive Pay and Positive Payee Tracking

A necessary evil of the AP staff’s day is reconciling cashed check payments against the issued payments in order to catch and prevent instances of fraud. Typically, banks will match client records against their own to determine if the account number, check number, and number of recently-cashed checks match up—a process known as Positive Pay. A related process, Positive Payee, tracks that same information along with the customer’s (payee’s) name, which creates another layer of security. Some banks don’t offer Positive Payee tracking, which is a shame. In those cases, if a fraudster washed the name on a check, but kept the other information the same, the fraud would be undetectable until the intended recipient claimed no-receipt. Some providers offer Positive Payee tracking as a service, so be sure to ask if yours does.

At the end of the day, your company’s security standards will always evolve to protect against ever-shifting fraud threats. It’s important to find a provider that can scale to meet those changes without sacrificing your high security standards. While fraud prevention remains a priority, it’s also important to know how your provider handles fraud instances and repairs damage.

If you're already searching for a payment automation solution, take some time to

Accounting • Auditing • Small Business