



## Fraud: Stop Thinking it won't Happen to You

**Executive Summary:** Fraud is a real risk to businesses and most do not realize they've become a victim until it's too late. There are simple controls to put in place to help prevent it, or perhaps bring it to your attention. Learn preventative measures and examples of embezzlement techniques.

**"No, that couldn't happen here."** "We have great people. They've been with me forever." How about "I worked with these guys for years at that other company and it's all good."? You know how many times I've heard things like this? I don't know, maybe from over 15 companies in the last year alone! Trust. Me. It can happen to you.

**The Heist.** Fraud or embezzlement happens numerous ways, here are some common ways:

- Fake invoice (accounts payable) – the accounts payable clerk creates a fake invoice to a fictitious company. This payee "company" somehow ends up being the clerk or a party related to the clerk.
- Vanishing invoice (accounts receivable) – payments may be diverted to a phony account and invoices are removed from the system
- Payroll – paying the wrong pay rate, paying too many hours, paying for non-existent employees, or paying for an employee no longer with the company.
- Selling company assets – if assets are discovered on a jobsite such as natural resources (gravel or dirt) or house furnishings (in the case of a refrigerator in a house demolition), these can be sold by employees for individual gain.
- Salvage – related to the previous item, there can often be precious metals (like copper wire from light pole to light pole) or just common steel or timbers that have value in the community or at a recycling plant.
- Property use – land owned or rented by the company for a particular job can be leased out to the "landlord" who is your employee (for example, on a camp job where workers need land to lease to park their trailer – this property is being leased by the Company from a lessor, but tenants unbeknownst to the Company are paying your employee since he has advertised himself as the landlord). A second example which is common is use of the Company's construction equipment on side jobs for which the Company has no knowledge and has not approved.
- Fuel – using company fuel cards to fuel personal vehicles (their own personal vehicle or their friends'). See My Story below.



**Preventative measures.** Here are some suggestions to combat fraud and embezzlement:

- Separation of duties – split duties to multiple people
  - whomever cuts the checks (or signs the checks) should not balance the bank account

*Scott Jennings, P.E., is the President of SJ Construction Consulting, LLC [[SJCivil.com](http://SJCivil.com)]; (808) 271-5150]. He recently owned and operated a heavy/civil construction company and now provides cost estimating, litigation support, and efficiency advice to contractors. He is the founder of Runjob Software, Inc. ([RunjobSoftware.com](http://RunjobSoftware.com)).*



- the person entering the invoices into the system does not issue payments
- the person opening the mail does not make bank deposits
- Password protection – keep passwords protected to non-fiduciary (it should go without saying that accounts with fiduciary institutions should be protected) websites that provide things like:
  - office supplies
  - general merchandise
  - food
  - airlines
  - other travel accommodations
- Asset reconciliation
  - fuel bills – generate an estimated monthly usage of fuel, jointly with the fuel cardholder, and monitor it monthly (or weekly!)
  - hard assets – generate a system of regular “asset check-ins” where employees are required to report the whereabouts of equipment (of course this is at Runasset.com)
  - bank accounts – account for cash use on a monthly basis
  - petty cash – if small amounts of cash are kept on hand, make sure to have simple accounting in an envelope or cash box

**My Story.** It started for me with an employee booking a trip to another state without my permission. She went into the airline website and booked a ticket for the weekend.

A far more serious case was when I learned after months of abuse that my employee was going to the local fuel depot, of which we were a card-carrying member, and having his friends pay him cash to fill up their vehicle. The rough scheme was to put \$100 of fuel in the fishing boat owned by the “friend” and have the “friend” only pay \$75 in cash to my employee. The friend saves \$25 and my employee pockets \$75; I paid \$100 to the fuel company. This loss was north of \$65,000 for me.



Finally, I had a project in which the earthen material being excavated was of value (it was winter and rainy, and this was gravel coming out of our site which was good in rainy weather). The buyer’s attorney called me one day and told me what was going on (that my employees were preparing to receive personal checks each around \$20,000 from the buyer). I was able to get the check for over \$40,000 cut to my Company (instead of my employees).

Each of these parties are people that I trusted and knew “well”. The airline gal I saw every day, the happy-go-lucky fuel theft came to our holiday parties with his, and finally the gravel guys were part of executive management.