



Contractor learns hard lesson

**By Mandi Lindsay
FCA Executive Director**

Greg Layton, FCA immediate past president and president of Western States Framing, has learned a painful lesson. Layton hopes by sharing his story that other businesses large and small, construction and non-construction, can glean wisdom from his folly.

Last May, Layton was in the market for a new key employee/office manager to be responsible for accounts payable, accounts receivable and more.

Layton received 81 resumes for the open position and through process of elimination and a series of interviews narrowed the scope to three finalists. Ultimately, Layton and colleagues opted for a designer-dressed, articulate and seemingly competent candidate. Layton and company, including the outgoing office manager, were so impressed by the candidate's professionalism they skimmed through her references and made only one call to inquire of this woman's bona fides. Layton's call to her reference was later determined to be a phone call to the candidate herself, so she could deliver a rave review on her own behalf.

The new hire excelled through her 20-day training period and over the following 30 days, rose to the company's key employee. But 45 days into her new job, she resigned.

Per usual in a job that deals with accounting and human resource issues, the new hire was afforded access to payroll accounts, employee personnel records, company financials and much more. So it came as quite a surprise that the woman was actually far more talented at another skill she had honed – that of professional thief.

The first clue that something was amiss came to Layton's attention the day before the bedazzling candidate exited stage right. Layton had gone to make a purchase on his work credit card and was puzzled to discover it declined.

After calling the credit card company, Layton discovered the company had placed a hold on his card because Western Union wire transfers, clothes purchases and more had been attempted. In fact, the credit card company had told him the previous 10 attempted charges were, by their estimation, bogus and they assumed the card had been compromised.

Layton knew the card had never been out of his possession and knew the card number had either been stolen from a previously patronized location or from someone at his office.

A path of flashing red lights leading to the new employee didn't sound, however, until the next morning, when a tenured employee called Layton and said he was having difficulty getting his checks cashed at the bank. The branch manager informed Layton that money had not been deposited into the company's account. By the time Layton got to the office, the employee had vanished and was effectively on the run, leaving only her keys behind.

Layton immediately called the police and put his IT team to work to secure the company's computer network.

It didn't take long to discover that the employee had stolen and exploited Layton's social security number by applying for and then using credit cards in his name.

"She was applying for credit cards online in my name and getting the approval in two hours time. She would then hijack the mail to ensure possession of the cards without arousing suspicion. She had already received two and ran them up to almost \$9,000 apiece. A third credit card arrived in the mail the day she left," Layton recalled.

Layton admits the hire's sole focus, and one of the easiest ways to commit theft, was to abuse credit cards.

"She had good, personal information and could achieve her objectives more under the radar than from stealing from the company directly," said Layton.

She stole company checks; she had an additional set printed with the company's information. And according to the bank branch manager, who Layton had befriended during the process of unraveling the crime, the employee was turned away from the bank the Friday before her abrupt departure for trying to cash a \$6,000 check with an unmatched signature.

Furthermore, the woman, with her out-of-state driver's license and Georgia references had a silent partner in Atlanta.

"In fact, as I was talking with the credit card company, they were telling me that charges were trying to come through from Georgia as we were speaking," said Layton. "Typical items charged included clothes, plane tickets, fast food, cell phone bills and much more. The majority of charges were for everyday types of purchases."

The woman is still on the loose despite having a warrant for her arrest. She is accomplished in hiding her real identity under a layer of aliases.

Layton admits that a more energy invested on the front-end would have eliminated the almost-debilitating lost time. Layton has since changed the way he does business and cautions other employers to learn from his mistakes.

"We've been in business a long time. Gone are the days when we used to hire people, put them to work, pay them and say thank you. Today, we have to worry about the criminal element," said Layton.

In fact a simple \$200 background check would have immediately revealed the social security number the employee used belonged to a boy in Georgia.

A very surprised boy, Layton said, after he called him up and gave him the dish on the woman and her antics.

"Today, as a company, we invest the \$200 for a background check and evaluation test offered through fellow FCA member Star Leadership. The results offer us a well-rounded look at our candidate," said Layton. "Additionally, we call multiple references and we don't give any one person carte blanche."

The woman got away with about \$15,000, which the credit card companies and retailers. Layton estimates his company lost \$7,000.

"This all went down effectively in less than 30 days, the lady we got was and is a professional thief. I can't emphasize enough that serious financial damage can be done in as little as 30 day's time," said Layton. "Take the time and protect your company."