

## Small Fraud Checks Can Result in Large Savings

Many people have been or will be the victim of a wrong phone number call in their lifetime. Most of the time, the caller dialed the wrong phone number by accident because they were unable to read someone's handwriting or their own, they were accidentally given the wrong number or the caller tries to remember the number without looking it up. But what if the wrong number wasn't so wrong after all. These seven digits or more if dialing internationally are arranged in a specific order to land a caller with the correct person or business on the other end of the line. This is similar to a routing number or account number in the business world. A specific number to send funds rather than voice messages from point A to point B. Someone wouldn't want to accidentally misread their handwriting or flip numbers around because the money will end up in the wrong place and not with the customer. But there are scenarios out there where that is exactly what someone wants to happen. They want money to go to the wrong place or if it's looked at from their point of view the right place.

These fraudsters are trying to integrate their way into businesses anyway possible. "Business fraud is ramping up; it is getting much worse," said the presenter of NACM's webinar, "Integrating Fraud Detection in the Credit Check Process." According to the presentation, manufacturing/construction and commercial services saw a huge uptick in targets from 2017 to 2018. The webinar reviewed several different ways to help combat fraud at the early stages during the check application and decisioning process. These different checks are something that's easy to do to benefit the companies and credit departments.

One of the first red flags a creditor should see is, "A lot of times, not always, fraudsters are in a hurry. ... If it's too good to be true, it probably is," according to the webinar. If there's a fraud protection process in place at the beginning of a new credit application, there's a better chance to catch any mistakes or attempted fraud. "Fraudsters are getting much more sophisticated, so creditors must do their due diligence. ... [They] need to raise to that level of sophistication as well," the presenter said. Over the last two years, their firm saved more than \$750,000 by implementing the smallest of changes. "It makes the credit people look like superheroes."

They are not so much changes as they are performing different checks to make sure items on the credit application are legitimate and true. When a company receives a new credit application, look at the email address and send an acknowledgement email. Another red flag is the email address itself. If a large company requests credit and the requestor is using a domain such as Gmail or Yahoo and not a typical business email address format, e.g., johnsmith@company.com, some questions should be asked. Another issue with emails is the changing of the domain slightly so it doesn't represent the actual email, e.g., johnsmith@company.com. This is business email compromise, and it is a \$26 billion scam, according to the FBI. Doing a fraud email check can be as simple as looking at the email and making sure it's right.

Online tools, such as whois.com and the Secretary of State websites, are great ways to find additional information. Even an internet search of the company using Google Maps or similar application can benefit credit departments. Searching the physical address of the company can also prevent fraud. If it's supposed to be a grand office building but the result of the search comes back as a dilapidated farmhouse, that should be a sign for further investigation.

Not all fraud can be prevented, but having small checks in place, such as reviewing emails and performing internet searches, can be a huge benefit for credit departments. There are also hidden savings by doing fraud checks. Companies can save on insurance premiums as well, noted the speaker.

—Michael Miller, managing editor