For Oklahoma Bankers Association – April 2016 issue
Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services, LLC

Business client article

What's in Your Mail?

Mailing correspondence, paying bills, and sending out marketing; it's all in the day in the life of a business. But what if your mail ended up in the wrong hands? That's an unfortunate reality for businesses across the country every day.

Brazen criminals are boldly walking into businesses, particularly those located in complexes, walking straight up to the front desk and taking outgoing mail right off the front desk. That quick. And they are rarely seen doing it. It's believed they stake out businesses, walking through and looking to see if anyone is hanging around the front area before they strike. When no one is around, they walk up and take anything of value. One receptionist had her personal cell phone stolen along with the company's outgoing payments that were waiting for the mailman to pick up.

So stop and think what was in your outgoing mail today? Checks? Anything with credit card or account numbers? All valuable details to a crook.

After stealing the outgoing mail, they create counterfeit checks using your business's information. They also "wash" the stolen check using a common chemical I bet every woman has in her closet. "Washing" the check means they removed who you wrote the check to, added themselves (or someone else), then cash the check.

With counterfeit checks in hand, the criminal group then recruits homeless people in major cities, cleans them up, and sends them into banks and check cashing facilities to cash the checks. At the first sign of trouble or a suspicious teller, the criminals who are part of the ring (sitting in the car) bolt, leaving a clueless homeless person inside. I say clueless because they don't know anything about the people they are cashing the checks for; all they know is they got a free meal and some money out of the deal.

This form of fraud has been going on for years and shows no signs of slowing down. It's happening all across the country, to businesses in big cities and small.

Here are a few thoughts from this security girl that I hope you will consider:

- **Hide that mail!** – Consider having the office "drop spot" for outgoing mail behind a locked door, or at least inside your business, away from easy preying at the front desk. Please don't stack it in hallways, mail rooms of large buildings, etc. Let's not make it easy for fraudsters!

- **Keep it hidden!** - I am here to tell you some people will steal anything. When I worked at the bank (many years ago) we had a chair stolen from a branch lobby.

(Yes, you read that correct – a chair.) Seriously, if it isn't nailed down, some consider it fair game. So be sure anyone sitting at the front or near the entrance to your office understands they should keep valuable items locked up at all times. That includes company property, and personal items such as purses, cell phones, laptops, etc.

- **Use Positive Pay** – Ok, so Positive Pay won't stop a bad guy from nabbing your account info, but it will stop you from taking the brunt end of a large loss and the hassle of having to get checks returned. If you can't feasibly work with Positive Pay for some reason, talk to your bank to see what other options exist.

- **Take it to the Post Office** – Consider taking your outgoing mail directly to the post office. Years ago I would have suggested drop boxes, but criminals are known to put glue or chewing gun on the end of a stick to fish mail out of these boxes. If you opt to use a drop box, make sure it's one in a heavily populated area where someone would be less inclined to go fishing.

- **Check those accounts** – Online that is. And daily. This is one of the best ways to catch fraud. A quick peek at your account activity will help you quickly identify if there is a problem, like counterfeit checks for thousands of dollars each hitting your operational or payroll account.

- **Stay educated** – Talk to you bank; they may have alerts available for customers either on their website or via an email service. If not, or you just want more information, register for one or more free services that will keep your business in-the-know about frauds that could affect you. I personally suggest looking into:
    - BBB Scam Stopper
    - FBI Scam Updates – right side of the page, click on "Get FBI Updates" to register for updates sent to your inbox.
    - USA.gov – very bottom of the page, on the right, click on "Get Email Updates on this Topic" to register for updates sent to your inbox.
    - Your Attorney General's website. Some AG's websites are consumer-centric, but others offer business fraud alerts. Depends on the state and their focus.
    - fakechecks.org – great training materials, including videos to test your ability to spot a scam.

These simple steps could one day save your business thousands of dollars in counterfeit check fraud losses. Simple security changes pay off big time.

About the Author

Rayleen is the CEO of RP Payments Risk Consulting Services, based in Orrick, MO. She travels the country presenting at fraud, payments and security conferences on topics

ranging from Mobile, fraud, risk management, and information security. Rayleen has been writing and presenting for 9 years. Previously she worked financial crimes investigations for a community bank.