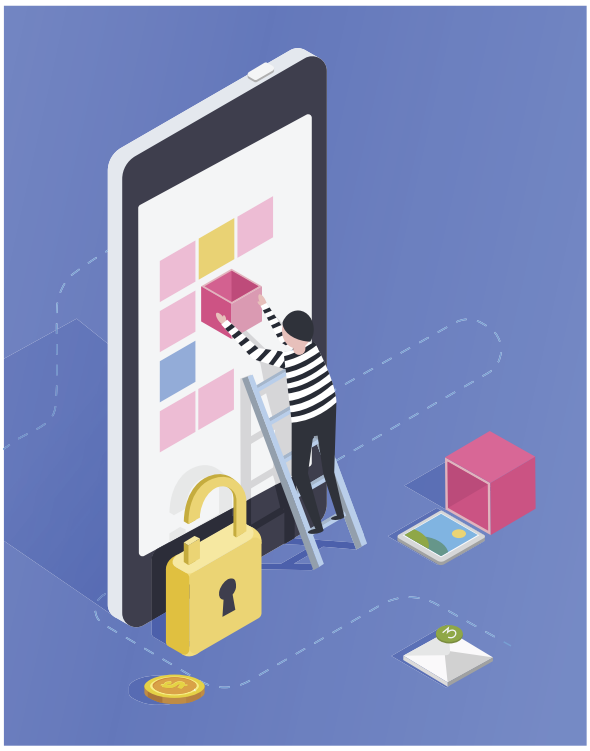
Money Mules, a Scammer's Best Friend

BY JON BELL

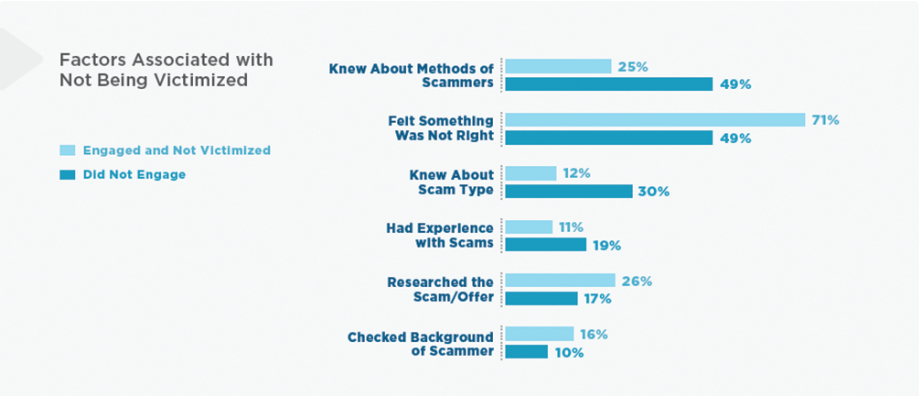


According to 2019 data from the Federal Trade Commission (FTC) released in January, Delaware has the dubious distinction of being 3rd worst in the nation for its number of fraud reports, and 7th worst in the nation for identity theft reports per capita. This is not the sort of list any state wants the honor of topping, especially since the FTC goes on to reveal that 23% of those fraud reports led to a monetary loss.

But as bad as the direct losses are to phishing emails, robocalls and the like, there's another kind of victim of fraud and scam in Delaware that doesn't get as much attention: money mules. Much like a "drug mule" is used to unknowingly smuggle illegal drugs over a border, money mules are used – also usually unknowingly – by organized scammers to launder stolen money, allowing the crooks to profit from their illegal activities while safely shrouded in anonymity. For scammers, it doesn't do any good to steal a credit card number or dupe someone into sending them a check if the crime traces back to them. They don't want to be caught, and so enter a money mule.

Here is one of the ways it happens in Delaware. A Smyrna woman falls in love online, and her beau (who's overseas, of course) invites her to help him with his real estate business. She opens a PO Box and a bank account, and he has all of his "clients" (read as: victims) send their check payments to her. The victims think they're renting a house in Rehoboth Beach for a week this summer, but they're being deceived – the scammer doesn't own the property. The scammer tells his romance victim to wire transfer him 85% of the money, but to keep the rest, because he loves her. So she happily continues collecting stolen money, depositing it into an account with her name, and then wiring the lion's share of it to her can't-quite-return-to-the-US-yet fiancé.

Or it might work this way. A recent college graduate in Wilmington sends out his resume, and – what luck! – an international fulfillment company that works with Amazon wants to talk to him about a work-from-home opportunity. The company's website is professional-looking and has that little lock everyone wrongly believes means the site is safe, and after a few emails are exchanged, the candidate is set up with a Google Hangouts interview. A faux interview ensues, followed by congratulations and an offer letter!



Reprinted from Exposed to Scams: What Separates Victims from Non-Victims? (p 11), by FINRA Investor Education Foundation, BBB Institute for Marketplace Trust and Stanford Center on Longevity, 2019. Retrieved from https://www.bbb.org/exposedtoscams.

These jobs go by many titles like Logistics Expert, Merchandising Manager, Package Processing Assistant, Fulfillment Inspector. But no matter the title, the responsibilities are the same: receive packages and open them, take a picture of the electronics inside (it's usually electronics), upload the picture to the "employer," download a new shipping label and reship the electronics off to their final destination.

The Wilmington victim was offered $20 per package he'd process, with bonuses for quick turn-around, and penalties for delays. At five packages per day, he'd be making $500 per week, and he quickly asked for more than five packages.

For a time, the job seemed real. The victim's online portal showed an ever-escalating balance, the "employer" was responsive to questions, and everyday more packages arrived. And then the police arrived because all the shipped goods were stolen and bought from online retailers with stolen credit cards. Oh, and the $20 per package? That was a lie, too – the victim had been working for the scammers for free and accruing real-life debt for the weeks he thought he had a job.

Money mules don't tend to go to jail. Law enforcement understands that most of these people are unknowing victims, and provides a warning letter that basically says, "You didn't know this time. Now you do. Do this again and you're complicit."

This kind of scam has a huge negative impact because not only do the victims lose but also it helps the scammers win. Victims lose their time and frequently suffer emotionally, either ashamed that they were deceived, angry that they were used, or worse. Meanwhile scammers are rewarded for their success with their anonymity intact and immediately start sourcing new money mules.

Better Business Bureau (BBB) receives these reports regularly, and while BBB works to shut down the scammers' websites and help victims, what's equally important is the education and outreach to warn about these and other scams targeting the local community. According to BBB's international research, the top two reasons why individuals targeted by scams don't engage (and so aren't victimized) are:

- Because they knew beforehand about the methods of scammers
- Because they felt something wasn't right

Spreading the stories of what scammers are doing locally reduces the risk that people will engage when the scam call, email or letter targets them. Reducing risk will reduce losses.

To report a scam that targeted you or your business, visit ScamTracker.org.

Jon Bell is the Director of Business Relations at Better Business Bureau Serving Delaware.

Better Business Bureau Serving Delaware

Money Mule:

Someone who (usually unknowingly) transfers illegally obtained money or goods to a scammer, allowing criminals to launder stolen funds while remaining anonymous.

How it Happens:

Scammers don't want to get caught. So when they buy goods with a stolen credit card or defraud people into making payments that aren't really owed, they can't receive the money directly.

Scammers look for people they can dupe into helping. Typically they trick people into thinking they're in an online relationship (a Romance Scam), or they convince people that they're being hired for a work-from-home job (Employment Scam).

The crooks then get the money mule to either open a bank account to receive stolen funds, or ship goods bought with stolen credit cards to the mule.

The money mules are then instructed to wire transfer most or all of the funds to the scammers, or else re-ship the stolen goods to a new address where the scammers can safely retrieve them. The scammers keep this up for as long as possible.

By fooling people into forwarding stolen money or goods to them, scammers cover their tracks and become that much harder to find and catch.

bbb.org

BBB