FRAUD TALK – EPISODE 97

Combating Increasing Fraud During the COVID-19 Pandemic

In this episode of Fraud Talk, ACFE Training Director Jason Zirkle, CFE, discuss the most common fraud schemes that arise during a natural disaster and, more specifically, which scams have emerged as a result of the COVID-19 pandemic.

Transcript

Emily Primeaux: Welcome to this edition of *Fraud Talk*, the ACFE's monthly podcast. I'm Emily Primeaux, Associate Editor of Fraud Magazine, and I'm joined by Jason Zirkle, the ACFE's training director. Thanks for joining us, Jason.

Jason Zirkle: Thanks for having me.

Emily: Great. We're in a unique position today because we're going to talk about disaster fraud as the world deals with the COVID-19 pandemic, and while much of the conversation deals with the spread and fallout of the disease, we're going to discuss how disasters like this are ripe for scams. It's not just pandemics, but also hurricanes and tornadoes and such. Let's start more general and talk about why fraudsters target the vulnerable during times of natural disaster.

Jason: Sure. The first place we got to start is focusing on serial fraudsters. Serial fraudsters, they think differently than most of us. At some point in their criminal career, they've overcome that idea of guilt and having to rationalize their bad behavior. They do nothing but sit around and try to come up with ways to defraud people. The issue with disaster fraud is that it becomes this perfect storm. You have these guys that are doing nothing but sitting around and trying to come up with ways to defraud people. Then now you have a situation where people are looking the other way.

Governments, law enforcement, regulators that may have some say in overseeing fraud controls in companies, all those people are too busy dealing with the disaster to temporarily worry about fraud. Then you have us, the consumers, and most of us probably feel like we're pretty savvy at spotting that fraudulent email. We live in those days where the Nigerian prince email scam, we've grown up with that. We normally think of ourselves as pretty savvy, but in the times of a natural disaster, we are focused on something else. Maybe we're focused on having to put food on the table, or where we're going to live if there's been damage to our home, so we are no longer thinking about fraud.

That is the perfect time for these fraudsters to strike. These people again, they think differently than most of us. They have no problems defrauding elderly people. They have no problems defrauding normal people that are in a very vulnerable state, so this just becomes this perfect storm where it's a great time for the fraudsters to strike because we're looking in the other direction.

Emily: Yeah, that makes sense. What kinds of fraud schemes are these criminals thinking about while the government is looking the other way? What are they thinking they're going to do to the vulnerable?

Jason: When it comes to the serial fraudster, we're probably going to get into a couple of different — I guess you would say “types” of fraudsters — but the serial fraudsters, the guys that are doing this year-round that are already committing fraud, they're going to do all the same things that they're already doing that we're familiar with. They're just going to ramp them up in the aftermath of a natural disaster. We're talking like the identity theft, phishing, when they induce you, they send you an email that's unsolicited and they trick you into clicking a link, and that link will download malware onto your computer that may steal email credentials or steal information off your computer.

Then you have social engineering where they call you and they pretend to be somebody else. Let's say it's the “grandchild in need” scam, where they call an elderly person and say, "Hey, Grandma, this disaster is really…I can't get home. I need you to send me money."

Then you've got charity fraud. You've got guys that are out there that are purporting to be soliciting donations for a charity that is bogus. All of these types of fraud that they're doing normally are just going to be ramped up during a natural disaster. Now they have this great reason for you to be more vulnerable.

For example, with phishing, you've got a lot of consumers that are out there and they are wanting news on the disaster. They're wanting news, for example, right now, in the COVID-19 epidemic, people are wanting to get news on what's happening in their areas, so it's a great time for a fraudster to send you an email, saying, "Hey, click here for news on coronavirus infections in your area." Then you'll click the link and it'll download malware. Again, all of the normal types of fraud you see like identity theft, phishing, social engineering, cyberfraud are there. They just now have an even better way of defrauding you and getting you to click that malicious link in the aftermath of a natural disaster.

Those are the serial fraudsters, then we can move on to other fraudsters, like contractors. Now, usually with contract fraud, this is going to apply when you have property damage, not necessarily COVID-19, but let's say an earthquake or a hurricane, and that's just when a contractor lies to you about the amount of damage on your home in order to sell you services that you don't need. We have serial fraudsters, we have contractor fraud…insurance fraud. This is the other side of it, when the consumer themselves looks at the situation and sees an opportunity to commit an individual fraud. What they'll do is they'll submit a fraudulent insurance claim and overstate the amount of damage that was done to their home.

In addition to all that, you also have corporate fraud. All the corporate fraud that we already have to deal with like misappropriation of assets, payroll schemes, those are all also hyped up during a natural disaster because operations for the company may not be what they normally are. You may have people working from home, so fraud controls start to fall by the wayside. There's so many different directions that fraud can come from after a natural disaster.

Emily: It sounds like a lot of fraud schemes we see in everyday life, but just really ramped up because of the times.

Jason: Absolutely, absolutely. That's what it is. It's people saying, "Hey, operations are not normal right now for the company. I think I can probably get away with stealing inventory." Or a homeowner says, "You know what? I'm probably not going to get this chance down the road. I can submit this false claim and get paid." A serial fraudster is going to say, "Hey, this is a great time to send malicious links out to people

because people are looking for stuff to click on." It just becomes everything that you already see with fraud becomes heightened after a natural disaster.

Emily: Yeah. You touched on a couple of potential schemes that people could see specifically during times right now with the COVID-19 pandemic, but could you go into a little more detail about how criminals are currently capitalizing on this disease and pandemic that has spread worldwide?

Jason: Sure. As everybody knows we're in the middle of this. COVID-19 has already changed the world. Most of us have not seen whole entire states issue shelter-in-place orders for their citizens. We're in unprecedented times. This is obviously the type of natural disaster that's not causing property damage so we may not see the insurance and contractor fraud that we may see, say, after a hurricane, but we've seen a huge uptick already and all of the other stuff like the serial fraud schemes.

One big one that's come about is phishing. The COVID-19 pandemic started back in December in China, and within a month, you had cybersecurity firms that were reporting malicious websites. I think one reported that there was over 4,000 new domain names registered that had something to do with coronavirus, and a majority of those were already getting hits as having malicious code attached to them. Then you had pretty early on too, I think in January, February, Kaspersky and a couple of other companies have identified these email phishing scams that purported to be from the CDC or the World Health Organization that were just getting unsolicited sent out to people. Telling people, "Hey, click here if you want information on the coronavirus."

The person would click on the link and then it would download malware, or it would have them rerouted to another website where they would enter their email credentials and their email address and their password. Then it would spit them out on to the WHO's legitimate website, so the person who clicked the link didn't know that their email address and their password was logged. They just got pushed out to the WHO's website, and they didn't know that the damage had already been done. The phishing has really taken off, and there have been quite a few new stories already out there with the phishing ramping up.

Another area for fraud, specifically right now with COVID-19, is the product scams. About two weeks ago, the Federal Trade Commission and the FDA sent letters to seven companies telling them, “We have seen that you guys are offering coronavirus-related products that appear to not be legitimate and you basically need to quit doing that.” This included sales of things like colloidal silver which is a supplement that many websites have claimed can cure coronavirus. You've seen other essential oils companies. People that are making bogus claims that these can treat coronavirus when in reality they cannot, so the FTC and FDA sent out those letters. Several of those websites, and particularly The Jim Bakker Show, he runs a radio show, were actually sued by several state attorney generals for the same claims.

In addition to the websites and everything, you have the legitimate websites like Amazon and eBay and even Walmart, their online store, where they allow third-party sellers to come in and sell products. They're having issues with third-party vendors selling products with fraudulent claims. I think Amazon have even reported that they've removed over a million listings for either price gouging or fraudulent claims. Those are some of the big ones we're seeing with coronavirus.

There's some others that we're not really getting concrete examples of, but I'm pretty sure they're happening. The corporate fraud that we talked about, business email compromise schemes, where in the aftermath of a natural disaster, or I'm sure it's happening right now, where the fraudster will identify somebody that works in the finance department at the company. They will send them a spoofed email purporting to be from the CEO or someone else and say, "Hey, you need to wire money to this account."

Then they send it out and then they don't get the money back. Only later do they find out that it was a bogus email. Social engineering, I know that's probably picked up even though we don't have any concrete examples of just people calling into companies, purporting to be from the CDC or WHO, requesting information.

Now, there is one that we have seen — investment fraud. A couple of weeks ago, the SEC sent out a notice, it was an investor alert. It was specifically on “pump and dump” scams and it correlated to COVID-19. What the investor alert said was, "Beware because we've seen at least two companies that are offering coronavirus-related products. Then you're going to have these brokers that will come in and convince you to invest in these essentially penny stocks for these companies that are offering these products. Then that will inflate the price of the stock. Then the broker, who also has stock, will sell it and make a profit. When they sell their shares, the price will plummet. That's a “pump and dump” scheme. The SEC has already sanctioned two companies for engaging in that behavior.

In addition to all that, again, I know this is a lot of fraud, a lot of information, but we're seeing a lot right now, but you have the fake charity and crowdfunding scams. In a natural disaster like right now, you're going to have serial fraudsters that are out there soliciting donations on behalf of a bogus charity. The problem is that these guys tend to be smooth talkers. They'll solicit donations either online or via the phone and they'll tell you a great story of their charity and everything that they're doing in coronavirus, but it's a bogus charity and they're just trying to get that money from you.

Again, with charity scams, do your homework. There are a lot of websites out there that you can check to make sure that the charity is legitimate. On top of all that, you have the price gouging. That's not necessarily fraud, but it's a form of fraud. It's basically, the illegal increase in price for services or for products that are necessary for coronavirus. You've got masks. You can have hand wipes, that kind of thing. There's been a couple of news stories about people that have gone out there and purchased up all of the hand sanitizer in a certain area, and they turn around and they sell it for ten times retail. Those are some of the things that we're seeing. The phishing is a big one right now, the product scams, the corporate fraud, the investment fraud, the fake charity scams, and then the price gouging.

Emily: You actually went into my next question briefly there when you were talking about charity fraud schemes, about how people can protect themselves and make sure that the links that you're clicking are legit and what they're asking money for is actually legitimate. Can you go into a little more depth on how people can protect themselves during these times and from these schemes? Because already people are feeling panicked and feeling like it's a dire situation. I'm sure that they're not taking that one second to look something up. Can you just remind everybody what they can do to protect themselves?

Jason: Yeah. A lot of this is stuff that you should really be doing in your everyday life anyway, but the biggest thing that most consumers can do is to just stay on top of their bank accounts and their credit reports. Make sure you're signed up for online banking. Monitor your bank accounts because if the serial fraudster targets you, and somehow accesses your bank account, they're going after your cash. That's what they want, so you just want to be monitoring that for any transactions that you don't recognize. My wife and I, we have online banking and probably about once every week or two, we're asking each other, "Hey, did you use the credit card at this retailer?" Anything like that, we're talking to each other.

Right now, it's a great time to do that. You get a lot of people that are sitting at home. Sure, a lot of us are busy, but you can't slack up on that stuff. This is exactly the time when you should be taking a little bit of time looking at your credit report. You've got websites like Experian that offer free services that will notify

you by email if any changes have occurred with your credit report. In other words, if a new credit line has been taken out in your name. These are the biggest things that people can do is make sure you're monitoring your bank account. Make sure you're monitoring any retirement or investment accounts. Then make sure you're monitoring your credit reports.

That's the first and foremost thing, but when it comes to all of this other stuff, phishing, for example, be wary of unsolicited emails. If you didn't ask for it or sign up for it, you need to be wary. Any emails from the CDC or the WHO, you need to be aware of the link itself. For example, if you hover over a link, you can see where that click is going to take you. A lot of people don't realize that but you can actually the link to have a different text than where it's going to take you. In other words, I can type in the text cdc.gov, but then I can go in and hyperlink that to a completely different website. The only way you're going to know that is if you hover over that. Make sure that you're actually going to the CDC's website and not some other website that looks unfamiliar.

Phishing, again, check the websites. Check the email addresses. Make sure that they're not slight variations of the legitimate like instead of cdc.gov, it's like say cdcinfo.org.That might be something that is not legitimate.

Don't click any links or attachments from unknown sources. Make sure before you click that link, if it looks like something that you did sign up for, you can hover over that to make sure that it's not taking you to a different space.

Product fraud, read through the seller's pages. Read through their reviews. Make sure that there a lot of people aren't saying, "Hey, this guy's a scam, a scammer. I sent him money, he didn't send me the product."

Beware of price gouging. Contractor fraud, again not necessarily for coronavirus, but in the aftermath of any natural disaster that's going to cause property damage. Make sure that you get at least three different bids from three different contractors. Make sure you do your homework. We tell everybody, trust but verify. I think one of the issues with contractor fraud is that you meet with a guy, and let's say he seems really great. He seems like his bid is pretty reasonable, so you decide let’s just go with him, but you didn't do your homework. You didn't look him up on the Better Business Bureau. You didn't look at him on Yelp. You just decided, "Well, I need to get that work done anyway, so let me just go there with this guy." It doesn't take that much effort to do your homework. Again, trust but verify.

The corporate fraud, any corporation that has fraud controls in place, don't ease up on those fraud controls. Again, your operations may have changed. You may have people working from home. This may be new territory for you, but make sure you're still focusing on those fraud controls.

And then, when it comes to insurance fraud, most insurance companies have already gotten pretty good at identifying fraudulent claims. A lot of that involves just focusing extra attention on these claims in the immediate aftermath of a natural disaster. For example, if an insurance claim is from a shop owner, and let's say their shop is only 500 square feet, but they're claiming several million dollars in damage for loss of merchandise, that might be a red flag.

With charities, it's the same way with contractors, do your homework. Trust, but verify. There's a lot of great websites out there like Charity Navigator that you can go to to research that charity and find out if it's legitimate.

Emily: Awesome. This is always the consumer can protect themselves, but we have at the ACFE, more than 85,000 fraud examiners worldwide. What can they be doing to help during times of a natural disaster?

Jason: First off, if you're a fraud examiner that's working for a company, let's say in internal audit or something like that, you should build this stuff into your fraud risk assessment and your fraud risk management program. You should already be thinking in terms of an event-type fraud like a natural disaster. Let's say maybe after a natural disaster, you reach out to key personnel and notify them, for example, about the dangers of business email compromise or social engineering and going through that training. There's lots of things that you can do at the company level.

Now, for just the community, I would just encourage CFEs to be more vocal in their community. For example, right now, we're all at home. We're all stuck. You can reach out to people in your community. You can start a blog. You can reach out to the city or the county and say, "Hey, we know that fraud is ticking up. Is there anything that I can do to help you guys put the word out about fraud in my community?"

I feel like there's lots of novel ways that you can think of. Put it out there on Nextdoor. Put it out there on social media. I actually just posted a few things on Nextdoor, warning my neighborhood of the dangers of fraud right now, and saying, "Hey, just make sure you're paying attention to phishing and you're not clicking on any links," and everything that we already talked about. Social media is a great tool right now to put that word out.

Emily: And just really educating people who may not see this and who don't know all of these ways to protect themselves.

Jason: Yeah, because if you've got people that are not really thinking about fraud in general in their daily lives, they're definitely not thinking about it right now. They've got a lot of other things on their mind. They've got kids home. They're having to figure out how to homeschool their kids. Their job is maybe in jeopardy. Fraud might be the last thing on their mind, but we need to tell people, "Hey, you're at home right now, go and start monitoring your bank account. Here's the link to Experian where you can sign up for a free credit monitoring. Here's the link to these different websites where you can read up on these types of fraud." Those are the types of things that people need to be hearing right now.

Emily: Awesome. Well, thank you so much for chatting with me this morning, Jason.

Jason: Thanks for having me.

Emily: This has been another edition of Fraud Talk. You can find all of the ACFE's episodes at ACFE.com/podcasts or wherever you get your podcasts. This has been Emily Primeaux, signing off.