FRAUD TALK – EPISODE 88

Fraud Is the New Black: 3 Frauds Perpetrated From Prison

In the most recent episode of the ACFE's podcast, Fraud Talk, Julia Johnson, CFE, Research Specialist at the ACFE, breaks down three recent case studies of frauds that were committed from behind bars. She explains how the schemes were perpetrated and what fraud examiners can learn from each case.

Transcript

Courtney Howell: Hello, and welcome to this month's episode of Fraud Talk. I'm Courtney Howell, the community manager at the ACFE. Today our guest is Julia Johnson. Hi, Julia.

Julia Johnson: Hi, Courtney.

CH: Julia is a research specialist here at the ACFE, and we have what I think is a very interesting topic to dig into. We're going to be talking about three recent fraud schemes that were committed from prison. Yes, the fraudsters were operating from behind bars.

First though, Julia, would you tell us a little bit about your role here at the ACFE, and also a little bit about your background?

JJ: As Courtney said, I'm Julia Johnson, and I work in the research department for the ACFE. I focus on accounting-related fraud and subjects related to that. So I update training materials on that topic and write different articles on emerging frauds and different fraud stories in the news.
Julia: Before I started at the ACFE, I worked in public accounting as an auditor. And prior to that, I worked in law enforcement for a little bit.

CH: Oh cool. What did you do with law enforcement?

JJ: So when I was working in law enforcement, I did civilian support type stuff. So I was processing paperwork for people getting arrested, and helping people get their property when they would get out of jail, and support the investigators in watching video surveillance, and just different tasks that they needed help with.

CH: Awesome. All right. So we're going to go ahead and dig in to our fraud schemes. So the first one, let's get into that one. And it comes to us from Ohio. What was going on in this one, Julia?

JJ: So this is actually a pretty interesting story. There was a couple inmates in Ohio that got caught for building two computers that they hid in the prison ceiling. This inmates had access to these computer parts through a program that they had at the prison where they would break down computers, old computers that people had donated to recycle. And they were given kind of lax supervision in this program, so during the times that they weren't supervised, these prisoners would steal the parts from

computers, build their own computers, and then were able to connect these homemade prison computers to the network and access all sorts of sensitive information and even the internet. They were able to access this by using the stolen credentials of one of their supervisors, who was in charge of watching them during this.

And when they were finally caught, the prosecutor's office did a full investigation and checked out the hard drive and what was happening. They realized that these prisoners were able to issue passes to gain access to different areas within the prison that they normally would not have been allowed. They were able to access inmate records, which contained sentencing information, social security numbers, lots of sensitive information that you really don't want anyone, including a prisoner, getting ahold of. They researched how to commit tax refund fraud using just a few elements, like social security numbers, date of birth, bank account information. And they also applied for debit and credit cards using other inmates' identities. And there was an application that they could also use to communicate with parties outside of jail. They also loaded movies and other media on thumb drives where they would sell to other prisoners in exchange for items that you could buy at the commissary. So there's a lot going on with this one.

CH: So I guess my first question is, how did they steal the supervisor's log in? How did they get ahold of that information?

JJ: So during the investigation, the prosecutor's office found one of the prisoners confessed to shoulder-surfing the supervisor, so just looking over his shoulder and seeing what he was typing, and the next day went in and used the same log in, and it worked just fine.

CH: Simple, yet effective.

JJ: Yes.

CH: Okay. So they were committing, you said, like false tax return fraud and then also credit card fraud?

JJ: Yes.

CH: So they were stealing people's identities. Did the other prisoners... I don't know if it had this in your research, but did the other prisoners know they were using their identities? Or they were just stealing them from the records that they uncovered?

JJ: They stole one prisoner's identity, and when he was questioned, he was not aware at all that this was happening. And when they asked the prisoner who was doing the theft, they asked him why he was chosen, and he said he picked this specific prisoner because he was young and had a long prison sentence, so he knew that he wasn't going to get out for a long time and that he would probably get away with it.

CH: Interesting. What are some controls that were maybe lacking at the prison? Like how could they have prevented this or even just caught it sooner?

JJ: Yeah, I mean, there's definitely a few things that could have been done to prevent this or catch it a lot sooner. One thing that they could have done is have proper oversight over the prisoners that were doing the work. The supervisor left them unattended for long periods of time, which gave them the

opportunity to build these computers. So I think proper supervision was definitely something that was lacking.

Another thing would be to maintain inventory records. So those computers that they were receiving, the donated computers, they should have been keeping inventory of the parts that were going in and out. They would have noticed that there was a lot more coming in than were coming out.

Also, a big one is to just protect your password. Know your surroundings. Update your password frequently so that if someone were to get ahold of it, it wouldn't be there for too long.

CH: That definitely would have helped. How long did this go on?

JJ: I want to say it was a couple months before it was discovered.

CH: So after they discovered that this was happening, what happened? How did they do the investigation? How were they caught?

JJ: The prisoners were caught because the network system at the prison alerted the technical department that the internet usage had reached its maximum for the day. And they thought it was kind of weird, because it was using some credentials that didn't work on the weekends, and this took place on a weekend. So that raised a red flag, and they went to check it out and found these two computers in the ceiling.

And they actually had two of the inmates take the computers down and put them in a supervisor's office. So the investigative process was not handled very well. I think they had the perpetrators taking them down. So one thing that could have definitely been done to protect that is just putting specific policies and procedures in place for... I mean, obviously this isn't a situation that you would probably have in a code of conduct type book. But just having specific procedures for handling suspected misconduct and things of that nature so that the investigative process can be as solid as it can be.

CH: Yeah. And I think one of the things that people learn as fraud examiners is, if there's a compromised computer, if you don't know how to handle it, you want to make sure that nothing is changed, nothing is destroyed accidentally, or intentionally in this case, if they're letting the prisoners or the inmates pull those computers down. So you want to make sure that someone is handling those who knows exactly what they're doing to preserve the evidence.

JJ: Yeah. It definitely should have been preserved. And if you don't, if you are going to touch it, or there's a chance that something could be disrupted, it's better to just leave it and make sure no one else touches it until someone who has that expertise is able to handle it.

CH: Yes. Exactly. So one reason we love looking at case studies like this and sharing them with our members is that there's always something to learn. So thinking about this on a wider scale, what can other organizations learn from this?

JJ: I think that other organizations can learn that... I mean, with the network access, and there was some alerts that it was trying to be hacked, and so I would just say companies should be aware that if they're receiving alerts that someone's trying to hack them, that it's not always external. It could be internal. So just keep an eye out for that kind of thing.

And if something seems suspicious, it probably is. So if there's red flags that are popping up, they should be investigated.

CH: What's really interesting about this, because I'm thinking about the fraud triangle now, was the opportunity that the inmates had. How did the fraud triangle... Like, what were the three elements that kind of like helped this scheme come together?

JJ: As we know, the fraud triangle consists of the opportunity, pressure, and rationalization to commit fraud. So in this story, obviously the opportunity was there, since they were given access, pretty much free reign to these computers. So that was the opportunity element.

I think the pressure came from... It could have come from numerous places. I think one of the pressures could be being released from prison, it's hard to find a job. And I think that this prisoner was maybe trying to just put some money away for when he is out one day. I mean, obviously it was by fraudulent means. Or just the pressure to have control again. When you're in prison, a lot of your control is taken away, so being able to do this and perpetrate this scheme, I think, might have given a little bit of control back, or the feeling of having control back.

And then the rationalization. I mean, they're already in jail, so... "We're already in jail. Why not commit another crime?" I think is probably the rationalization, if I had to come up with one.

CH: Yeah. Obviously we don't know for sure, but it's interesting to think about those different elements. Okay. So lots of good stuff to glean from that first case, but let's go in with our second one.

This one happened in Florida. And this one involves cryptocurrency and money laundering, so a couple different elements that are really big, hot topics in the news right now. So what was happening in case number two?

JJ: So this one is also another interesting one from jail. Inmates at the Pasco County Jail in Florida were having money deposited into their commissary accounts, which are pretty much debit cards for prisoners that they can use to spend money within the jail for different items. So they were having money deposited into these accounts coming from stolen credit cards. And the stolen credit cards were purchased on the dark web using Bitcoin, so they had co-conspirators on the outside that were helping them with this scheme.

So the stolen cards were purchased on the dark web, and then the inmates would have the funds deposited into their commissary accounts. And then once it was in there, the inmates would ask for their accounts to be released to the public, which is something you can do, have it released externally. And the co-conspirators on the outside would then collect these released funds.

So pretty much just a regular pass-through scheme. The commissary accounts acted as a shell company in this type of money-laundering scheme, on a smaller scale than some, but a shell company nonetheless. And these inmates were able to make deposits into their accounts using the stolen credit cards a total of 43 times. And one individual who was part of this scheme, who was on the outside, was arrested and is now facing fraud charges related to this one.

CH: Interesting. So it's interesting to compare the two. The first one, it was all internal. It was all happening within the prison, using the prison's internet and information from other prisoners to then commit frauds outside of the prison. And this one took some people inside and some people outside to work together to kind of make it happen.

So this was a money-laundering scheme, basically. Can you walk us through what money laundering is and how, in this specific case, it was perpetrated?

JJ: Yeah, definitely. So money-laundering is pretty much just where criminals attempt to take funds obtained from illicit sources, whether it's stolen money, drug money, just dirty money pretty much, and they attempt to disguise it as legitimate funds that they have earned and have a right to spend.

So there's three steps in the money-laundering process, and those are placement, layering, and integration. And so the first step, placement, is where the illegal profits are introduced to the financial system. So when the stolen funds were placed in the commissary accounts by the external parties, that was the placement. And in a traditional money laundering scheme, that would be when these funds are deposited into a bank account.

So then the next step, layering, is when funds are moved around to try to disguise the paper trail of money. So this is when the commissary accounts were open to the external parties. And in a bank, this would be making different deposits and withdrawals and kind of shuffling money around to different accounts to kind of try and break it up.

And then the last step, integration, is when money's integrated back into the economy. So in our example of this Florida situation, it would be when the co-conspirators were able to access the stolen funds again. So that would just be, in a bank type situation, when someone complicit in the scheme is able to take this money and then use it to do whatever they want with it.

CH: As you were explaining this, I was like, "Oh, it's kind of ironic that they're using a prison fund to clean their money." I don't know. Just kind of funny there. You wouldn't necessarily think of a commissary account as a place to clean up your money, but for these people it worked for a little while.

What about takeaways? What was missing? What were the controls that they could have had in place to prevent this?

JJ: I think it would be hard to kind of have a ton of controls over this, just because it's so brazen and, quite frankly, ridiculous that... I mean, I'm sure the people that found this were pretty shocked. But I think the number one thing that we can learn from this is to always go through your monthly credit card statements and just make sure there's no charges that you're not aware of. Regularly checking credit score to see if any new accounts have been opened in your name is another big one. And then if you do see that there's activity that you haven't done on there, then freeze those accounts really quickly.

CH: What about the fraud triangle here? How were the three elements coming into play?

JJ: I think once again the opportunity was there for them. They had this commissary account. I mean the opportunity to commit another crime.

CH: Did you know if the external people who were kind of organizing this, did they already know the inmates? Was it like something that they set up? Or did they approach them while they were imprisoned? Do you know?

JJ: It didn't say whether they knew them or not, but I'm assuming that the prisoners probably got some sort of kickback for helping these guys out.

CH: So maybe those relationships are something to look into as well?

JJ: Yeah. I mean, I think the pressure is the money. I think these inmates probably were getting some money back from helping them out. And when you're in jail, you're not making any money, so that was definitely a pressure.

And then rationalization, I think, once again, they're already in jail, so what's another crime? I'm already here. Or helping further another scheme could be another rationalization. And if they did know the people that they were working with ahead of time, it could just be like something that they're continuing, you know? So preexisting relationship that they want to continue.

CH: Definitely. All right. So now we're going to talk about our third case, which, our first two were more a group effort, and this one is more on an individual level. So what was happening in this third one?

JJ: This lady was committing healthcare fraud, got caught, and was sentenced to nine years in prison. She was stealing identities of counselors and billed the government for millions of dollars of psychotherapy sessions that never happened. So she pretended to be a counselor and would bill Medicaid for fake patients. And in this first scheme, she bilked Medicare out of more than $2,000,000 in false claims and used names of 500 fake patients, who were mostly children. So she was caught, sentenced to nine years in prison.

And in between the time she was indicted and her sentencing, she started her scheme back up again. And this time she recruited one of her friends. Her name was Karen Jones. And she needed some money for attorneys fees, so her friend agreed to help her do this scheme again. And so the friend owned a personal aid services company that was a provider in the Medicaid program, so she was receiving funds from Medicaid the correct way, the legal. But then she went around and started a shell company for the... Alexis Norman is the lady who was caught for the first scheme.

So the friend helped Norman open a fake company, a shell company, and opened a business bank account. They did the same method as Norman did before by stealing identities of Medicaid recipients to submit false claims. They actually obtained these Medicaid provider numbers from licensed professionals who responded to their job advertisements on Craigslist. And these counselors weren't aware that their information was being used in this fraud.

So the friend would go and withdraw money from this account of the shell company then go meet Norman for lunch and give her the funds. And this happened once a month for about a year. And she was giving her $9500 at a time, which some people might know as right below the reporting requirement for banks.

So when Norman began... She started serving her sentence, her nine-years sentence for the first fraud, and her friend opened up another shell company to do the same thing and raise some more money. She

would go visit her friend in prison and would wear red when visiting her to indicate if the claims had been paid. And they communicated through and the phone service of the prison to continue this scheme going.

And it wasn't uncovered until investigators and Norma's attorneys met to discuss a dispute over the losses of the first scheme. And she had given them some documents, and it had additional counselors on there. She had gotten mixed up in her schemes and put the fake counselors from the seconds scheme onto the documentation for the first scheme. So they realized that she had been doing this all over again.

CH: Oh my gosh. So only by a mistake did they find out it had happened again.

JJ: Yeah. And so after they realized that she had been doing this whole thing a second time, she really got the book thrown at her, and she received a 30-year prison sentence for the total schemes.

CH: Dang. Okay, lots to unpack here.

JJ: Yes.

CH: So one thing that caught my interest while you were describing what was happening was that they got provider info by a LinkedIn ad, right? Is that what you said?

JJ: Craigslist.

CH: Craigslist ad. Okay. And so providers were just giving them their info?

JJ: I think that they made it seem that they were legitimate, very legitimate. But I think that's one of the takeaways here is don't give out any sensitive information, whether your social security number, if you have professional certificates any of those numbers, unless you are 100% sure that this is a legitimate source, because you can make stuff look pretty on the internet and make things look real, but it could all just be kind of a scam, so.

CH: Yeah, maybe they should have done a little bit more research on what they were sending their information to. Did Karen Jones, the accomplice, did she get sentenced as well?

JJ: Yes. She received a prison sentence, and I believe it was around 60 months. So she didn't get as long as Norman did, but she still was caught up in it, so.

CH: Okay, so you said that she basically only got caught for the second one because of a mistake. How do you think this could have been prevented or caught, the second scheme or even the first one, sooner? What sort of controls should have been in place?

JJ: I think companies that are receiving Medicaid payments, or any government payments, should be subject to surprise audits or surprise visits. These companies that these two were operating, the two shell companies, had no employees and were providing no services, so had somebody gone to just even go check out the office, they would have realized there's nothing going on here. So I think just making sure that those people know that someone could drop in at any moment, so they better be legitimate.

Another thing too, I mean, if they had monitored her communications while she's awaiting sentencing for this fraud, they might have been able to see that something was going on too.

CH: And you mentioned that she made several withdrawals or deposits, I can't remember, that were just under the reporting limit? Is there anything that they could do there? Seems like it's really close.

JJ: Yeah. So the reporting requirement is $10000. So she was just right under there with $9500 withdrawals every month. And I think if banks are seeing some activity like that where it's a regular occurrence of somebody depositing or withdrawing just below the reporting requirement, that should also be noted and kind of investigated and looked into further.

CH: All right. Well that's our three prison cases. Thank you so much for sharing and diving into those with us today.

So if you enjoyed today's episode, be sure to check out our monthly Facebook Live series called Fraud in the News. Julia is often a host on there. We share current fraud headlines and, much like today, delve into what fraud examiners can learn from each one.

And remember you can find all episodes of Fraud Talk at acfe.com/podcast or wherever you listen to podcasts. This is Courtney Howell, signing off.