FRAUD TALK – EPISODE 110

Operation Trojan Shield: A Global Takedown

Operation Trojan Shield was a collaboration between the U.S. FBI and DEA, the Swedish and Australian police, and other global agencies to infiltrate an encrypted chat platform. The operation led to 800 arrests, seizures of drugs and firearms, and an ongoing list of money laundering revelations. In this episode, Mason Wilder, CFE, ACFE Sr. Research Specialist, and Mandy Moody, CFE, ACFE Communications Manager, discuss the "sting of the century."

Transcript

Mandy: Hello, everyone, and welcome to this month's episode of *Fraud Talk*. I am Mandy, the Communications Manager here at the Association of Certified Fraud Examiners. I am joined today via Zoom, even though we're actually both in the office, [chuckles] by Mason Wilder. Hello, Mason.

Mason: Hello there, my name is Mason Wilder. I'm a senior research specialist for the Association of Certified Fraud Examiners also here in Austin, Texas, with Mandy.

Mandy: We're going to dig into Operation Trojan Shield, also called the sting of the century. Do you think that's fair, Mason?

Mason: It's catchy. It was quite the law enforcement operation. It's pretty much a dream operation for a law enforcement agent.

Mandy: Yes, that's true. There are some fraud connections here that we'll get to. Let's just start at the beginning. The beginning of June, news breaks about 800 people being arrested in this huge law enforcement operation, and this is global. This was a joint effort, I think, started in 2019 by the Australian Federal Police and the FBI. Am I correct?

Mason: Yes, it was definitely a collaborative effort. The two main law enforcement agencies were the FBI and the Australian Federal Police.

Mandy: News broke. I've got it here. June 8th. What exactly happened? What did they announce to the world that had happened?

Mason: When it went big, that was the result of a worldwide two-day takedown of all these people that had been using these encrypted communication devices. It was 500 arrests across about 15 countries that took place over two days. There had been arrests previously associated with this investigation as they were carrying out the investigation. The event that really kicked it all off was the FBI busting a different encrypted communications network.

As they were carrying out enforcement efforts there, they came across a confidential human source who had been selling these devices. He told them he was involved with working on a next-generation device, and, basically, offered his services as an informant to work with the FBI to develop these devices, and he would sell them to criminal organizations worldwide using his already established contact list.

Mandy: Hold on, I'm going to stop you right there. Explain, just for everybody listening, what an encrypted device is.

Mason: There's a great deal of demand within criminal organizations and just worldwide organized crime for devices that are safe to use without fearing that law enforcement is going to be eavesdropping and spying on you. There have been several companies that have either modified existing smartphones or developed their own hardware that run encrypted communications networks that work like either email or chat and messaging platforms. The device is encrypted; the traffic is encrypted. They're only sold on the black market through word of mouth.

Criminals get to not using any kind of euphemisms and speak frankly about exactly what they're doing and how they're doing it and where they're doing it and when they're doing it supposedly without fear of law enforcement spying on that.

Mandy: They can safely conduct criminal activity?

Mason: Yes, theoretically. That's the sell for the organized criminals, but this was not the case with this one. The FBI basically created their own platform and got this guy to help distribute the devices, and then every single message or email that was sent, basically you were going to BCC someone on an email, it created a copy of every single message and sent it to a server in a different country. Then the Australian Federal Police would go through all those messages, send the highlights to the FBI and other international law enforcement agencies a couple of times a week.

A couple of years later, there's been 800 arrests. They sold almost 12,000 of the devices to people linked to more than 300 organizations in more than 100 countries. They've got 27 million messages or so that they intercepted to analyze and learn more about the inner workings of all these criminal organizations.

Mandy: I'll give a few stats here. You just said more than 800 arrests and the seizure of over 8 tons of cocaine, 22 tons of cannabis, 2 tons of synthetic drugs, 6 tons of other synthetic drug precursors, 250 firearms, 55 luxury vehicles, and over 48 million in worldwide currencies and cryptocurrencies, 16 countries, and more than 700 house breaches. That was a lot.

Mason: Yes, and it's clear not only from the reporting, but actually the FBI revealing it as well, this was primarily targeting drug trafficking. It was an operation from the Organized Crime Drug Enforcement Task Force, and they were keying in on international drug distribution networks.

Mandy: As far as the encrypted communication that they did use and the data that they had, any insight into how they even went about combing through all that data?

Mason: There's some software that you can use for link analysis and stuff that has some artificial intelligence or machine learning capabilities so I'm sure there was some of that. Honestly, I bet there were a lot of Australian police officers just sitting around getting a big kick out of reading all these messages and, "Hey, hey, come check out what this guy said."

Mandy: It says a lot about countries working together and law enforcement agencies coming together. The one article that I was looking at, actually it was Europol's announcement, it had, obviously, the U.S. FBI, the Swedish Police, the Netherlands, Australia, Europol. Something that we hear a lot from fraud investigators is getting that cooperation across the border. I imagine if they would've done this on their own, it would've only impacted one or a couple of countries, but working together, they were able to bring down a much larger pool.

Mason: I imagine it's pretty easy to get the cooperation of other countries' law enforcement when you hand them a warrant on a silver platter, like, "Hey, I've got these messages specifying exactly what this guy purchased from another one for how much money on what date, and here you go."

Mandy: What do you think fraud examiners can learn from an operation like this as far as a true undercover making the technology that you'll bring somebody down with?

Mason: It's tough for me to imagine a scenario in which fraud examiners would be able to provide some kind of technological tool that they could then use to surreptitiously find out everything that another fraudster was doing, but hopefully, there will be some impact to facilitators of fraud like the money launderers.

One thing that I'm sure the law enforcement agencies are going to be sharing are some people that were specified in the communications or referred to, like criminals saying, "Hey, this guy can help you clean

your money. Here's his contact info, reach out to him," or discussing different methods of money laundering or jurisdictions where it's easier to launder money.

All that kind of information that they've gotten will be tremendously useful to them, I think, going forward in identifying money launderers and having more tactics and techniques in their book that they can reference whenever they see similarities in their investigations going forward.

Mandy: One of the recent arrests that just came out of that was someone in New Zealand charged with conspiracy to launder money, because of what came out of this, which I imagine, money laundering goes hand in hand with a lot of the money people were making?

Mason: Yes, that's why I think, I'm sure there were a ton of either tips or referrals amongst criminals on this network of like, "Here's what you do with your money." Or "Talk to this guy, he'll help you out." It'll be interesting; not that we'll necessarily see how they handle all that information or that they'll reveal it, but I wouldn't be surprised if some of those facilitators, some of those, the Panama Papers kind of lawyers, people that just have a whole business model on helping others move money internationally and avoid taxes or potentially launder money.

I wouldn't be surprised if they get targeted to reveal who all their clients are. For more drug dealers, I think the law enforcement is probably a little more interested in the organized criminals than the money launderers and so we might not see a cascade of money launderers getting arrested. That doesn't mean that law enforcement in those countries won't be reaching out to them to get a hold of their black books.

Mandy: Do you think this is a deterrent for criminals in the future to think twice that someone might be listening in?

Mason: Yes, absolutely. There was a similar operation, a very similar operation that was announced last summer, I think I wrote something about it in *The Fraud Examiner*, but it was targeting a platform called EncroChat and it was all European. It was mainly France and Dutch authorities that spearheaded that one. It was very similar, several 100 arrests, and it was proprietary technology. The app was called EncroChat. I think the devices were just called EncroChat devices.

Between that one, I think there was one other platform that got dismantled. I don't think it had been infiltrated to the extent that these two had. There's a big demand for these devices, but surely, after these three operations in just over a year, organized criminals are going to think twice about whether or not any device is truly safe, or they can really communicate freely on any of these things.

Mandy: What do you think or do you have any predictions for how they would communicate?

Mason: Just back to using the more common devices or regular off-the-shelf phones, but just using more code language and trying to talk about specifics only in person? I don't know. You can't really hide, I guess, would be the big takeaway from these guys. Certainly, if I was a member of an organized criminal organization, I'm definitely not believing anybody that tries to sell me a black market, encrypted phone.

Mandy: When I read stuff like this and even the EncroChat article that you wrote a while back, what's your go-to for learning more about the technology that is already here and even, it changes every day. How do you stay on top of it and how do you know what even to look for?

Mason: That's a good question. I don't think there's a super straightforward perfect answer. Not really to toot our own horns here, pat ourselves on the back, but just the other week when we had our conference going on, I remember looking at all the different sessions to figure out what to go back and watch after or listen to after the conference was over. We had a lot of really good speakers talking about different things, from artificial intelligence to cryptocurrency tracing and different cutting-edge prevention stuff.

You find somebody that knows what they're talking about at an event like that, a conference and maybe go see if they have a Twitter feed and follow that, see if they write articles for a particular publication, or

just do some searching on those different technologies. Anytime you find a publication that you got a lot of value out of a story they ran or something, maybe follow them or go check them out more regularly, subscribe to newsletters or things like that, so that you are regularly getting new information that's about different technologies and their implications or ways to leverage those technologies.

When you're having your cup of coffee in the morning, just go through your inbox for newsletters or news alerts and just make sure you're exercising your brain muscle and staying up to date on stuff.

Mandy: When I started working here, 11 years ago, I set up a Google alert for fraud and I still do it to this day. I really do comb through every alert about fraud because I needed to learn and understand that. I think that's something a lot of people have done too, is with different technologies or artificial intelligence or those different buzzwords that you can get the latest news on. I know you have a very meticulous way that you organize the stories that you see.

Mason: Yes, I do all kinds of dumb stuff and a lot of it is redundant. I just try a bunch of different things. I've got 10 million bookmarks in my browser. I've got a free database through Zotero, where I plug in a bunch of articles and tag them with just whatever stuff I can think of as I'm reading through it so that I can go back and reference that stuff. I've got those news alerts. I use RSS feeds. I have an RSS feed reader, all of that stuff. There's probably other things I could be doing as well, but that gives me more stuff than I have time to read really.

I really get the sense that they definitely know what they are talking about and explain things well. I certainly make a point to follow them on whatever, mostly Twitter or if they have their own newsletter or things like that. I look for experts that really do a good job of explaining things.

Mandy: One of our keynotes a couple of weeks ago, Amber Mac, has a weekly newsletter that breaks it down about latest technology and what's going on. It's super easy to read. I can just read the headlines. A lot of it is about AI, about data, but in a way that is actually fun to read and it gets the latest and greatest for that week.

Mason: To put this into more of an investigative context or an actual, practical context, if you're working on some kind of a case that involves some technology that you're not super familiar with, it really helps if you have someone that you trust, that you can reach out to and just tell them like, you don't have to tell them about the details of the case so you can preserve confidentiality or other legal privileges, but just ask them for a recommendation or a referral for an expert in that field.

If you've got somebody that knows tech and has a good rolodex, it's always good to have their number handy so that you can call them and get a recommendation because there are so many technical tools available and at this point, even the new ones, there's a lot of people out there working on solutions for better analysis or tracing involving all these different technologies. You don't want to miss out on leveraging those kinds of opportunities, just because you don't have time to fully understand that technology.

If there are distinct points, I guess, in any investigation involving a technology where it becomes imperative to involve an outside expert, somebody that really knows what they're doing, rather than you trying to figure it out in the course of an investigation. If you notice the suspect is converting fiat currency into cryptocurrency and you know they've got cryptocurrency, but you don't really know how to begin to trace it, that's when maybe call somebody that specializes in tracing that cryptocurrency so that you can really have a good chance of getting to the bottom of that, instead of trying to do it yourself.

Digital forensics is another one. If you think somebody is using their work phone for nefarious purposes, don't try and get all the data off of that phone yourself, just find somebody that really knows what they're doing, and pay them the money to get their expertise involved, you know?

Mandy: Yes. Well, this ties in nicely to the Operation Trojan Shield is. Don't be afraid to think outside the box. What the FBI did, and the Australian police, they didn't just learn technology, or learn encrypted communications, and try and piggyback on something, they actually created their own. I'm sure that was out of a lot of people's comfort zones, and to even begin that conversation of "Let's just make our own," and I'm sure that EncroChat helps, as more people are doing it. We can just create our own instead of trying to go and figure out a different technology, but really not being afraid to innovate, and go at it a different way.

I just thought that was really impressive because you always think, we go to so many different conferences, and attend so many different sessions that tell us we're so far behind the criminals, like, "We're trying to keep up, we're trying to keep up." "We've got to keep up with the fraudsters." But what they did was completely; they didn't just keep up, they did their own innovation and went around and then at the end of the day, they outsmarted the people who would always think are outsmarting the victims and us.

Mason: They caught up and got one step ahead.

Mandy: Yes. Which is such a happy ending for us, because usually, we're talking about the fraud that did happen, and how we missed it, and "What did you miss?" But this is a proactive story.

Mason: Yes, this was a big win. We'll continue to produce victories going forward, I think, for the law enforcement agencies involved because they've got this treasure trove of data and information about methods, individuals, they're going to be able to apply. They're probably going to end up arresting a lot more people that they just haven't gotten to yet but there also will be frameworks that they can apply to future cases.

Like I said, at the very beginning, it's like the dream law enforcement operation because they got a bunch of just unfiltered content from criminals all around the world and they know everything that they were saying to each other, and so there'll be just a ton of value for them to reap the rewards for a while, I would assume.

Mandy: Well, thank you for sitting down and talking about it. We wanted to talk about this. I know there's a very small fraud titan and it's a lot of drug trafficking and drug sales, but I think you're right, we'll continue to see money-laundering come out of this, just like with the Panama and Paradise Papers, they've got a lot to go through.

Mason: Yes, I think it's going to be really valuable. They just recently made the big takedown and announcement. I'm sure that there's lots more to come in terms of information sharing amongst agencies, and the money laundering thing will be the big link to fraud. I'm sure that FinCEN and some of the other international or national intelligence units, or financial intelligence units, will get some really good information out of this about very specific money laundering patterns that they can look for.

Hopefully, they arrest more money launderers and those facilitators of fraud so that it makes it harder for people to do the large-scale tax evasion and money laundering and just those financial; moving finances around illicitly all over the world. Hopefully, things get harder for them, just like it is now going to be a lot harder for international crime organizations to talk to each other securely.

Mandy: Awesome. Thank you, Mason.

Mason: Yes, anytime.

Mandy: Thank you all for listening today. You can find all of our episodes wherever you listen to your podcasts. You can search for *Fraud Talk* and hit subscribe. You can also find our collection at ACFE.com/podcast. That wraps up this month and we will talk to you again next month.