Adam Mazmanian:

Hi, everyone. My name's Adam Mazmanian. I'm executive editor of FCW, and thanks again for tuning in to the Government Executive Cyber Summit. The more recent adoption and widespread use of cryptocurrency has led to rapidly advancing threats, many of which span federal, state, and local law enforcement entities. We continue our agency spotlights with Bill Smarr, special agent in charge for the Dallas Field Office District in the US Secret Service to discuss how law enforcement can best navigate this emerging threat landscape. Hi, Bill. Thanks again for joining us today.

William Smarr:

Good afternoon, Adam. Thanks for having me.

Adam Mazmanian:

So I'm just going to dive right into the questioning. When people think about cybersecurity, I'm not sure they think Secret Service in the very next breath. What's the role of the Secret Service in investigating cyber crime?

William Smarr:

That's a good question, Adam. I think what you'll find with the Secret Service starting back in 1865, when the Secret Service was first founded, that was really, our main charge was to investigate at the time counterfeit currency. So along that same vein, we've always been involved in investigations even before our protection mandate came along in 1901. So from 1865 moving forward we've transitioned, evolved, if you will, through counterfeit currency then in the bank fraud, wire fraud, credit cards back in the '80s, and just continue to evolve into what we have now with. Anything that we do, touch, seems like in our everyday lives, involve some type of cyber-nexus, whether it's your phone, your computer, work, and then when that ties to money, that's why the Secret Service is involved. So we're really charged with protecting the US financial infrastructure.

Adam Mazmanian:

That counterfeiting mission is probably one of the oldest federal law enforcement missions there is out there. How did you get started and see an opportunity in cryptocurrency crimes?

William Smarr:

I think just that with our investigative history, we've always been an investigative agency. So as things evolved, treasury checks, and then as treasury checks turned into direct deposits, all that ties back to the US Treasury that were charged to protect. That's actually where we started back in the Department of Treasury back in 1865 and have since obviously transitioned to Homeland Security in 2003.

Adam Mazmanian:

Now, victims of cyber crimes don't really have... There's not like a 911, you can call and say, "I've been hacked." Who should people call when they're hit with a hack, or ransomware, data exfiltration, and specifically who should be looking to the Secret Service as a point of contact for reporting and requesting investigations of cyber crime?

William Smarr:

Well, I think any secret service agent or employee would tell you, we would love for you to call us, but we realize not everybody's going to call the Secret Service for every type of cyber crime or financial crime, they come across. So what we say in our mantra is to call somebody, call a member of law enforcement, hopefully somebody that you've had a preexisting relationship with, if you're a big corporation or a company that you have that built into your cyber incident response plan. But really, the Secret Service, our model is based off of task force model. So not just the Secret Service agents and analysts that look at this type of crime, but also our task force partners through our state and local officers.

We started our task force, specifically our electronic crimes task force back in 1995 in our New York field office, and that has since expanded to, we have 44 total across the globe; 42 of those in the US, and then 2 overseas. So really, when we say the Secret Service, even our task force partners that are in your own local communities, state police, local, territorial, tribal, what it may be, reach out to one of those, and more than likely, one of those folks that you're going to be talking to is somebody that has went through some training the Secret Service has provided.

Adam Mazmanian:

What kind of backgrounds or capacities are you looking for in these agents? If you're a Secret Service agent dealing with cyber crime, are you a coder, are you more of a investigator? What kind of technical shops do you need to do this job?

William Smarr:

I think as an agent, it is typically that good old fashioned police work, right? We're talking about cryptocurrency today, but really anything that touches cyber, at the end of the day, there's somebody behind the keyboard, and specifically with cyber and with crypto, what the Secret Service does is follow the money. So we're very good at following the money, whether it was a treasury counterfeit, or treasury checks back many years ago. The same thing goes on with cryptocurrency and the illicit money laundering that's attached to that. Obviously crypto is not illegal and it's face value, has very good purpose, and is used for some good things. But as criminals always do, they find a way to circumvent the laws, leverage that to launder their ill gotten games.

Adam Mazmanian:

We're in the midst of a kind of all government effort to crack down on cyber crimes, and there's been a flurry of activity in Congress regulatory activity to sort of say, "Well, who does what?" There are a lot of agencies with roles to play here. How do people know what rules to follow when it comes to their own cyber hygiene, their own requirements, and then I guess I want to ask you, too, your DHS sibling CISA is sort of at the center of all this. How do you see that organization developing as being the kind of quarterback for cyber issues government-wide?

William Smarr:

Now, I think you touched on it when you said whole of government. One of the ways I like to look at it, and when I talk to different groups, it's not just whole of government, it's really whole of society from that online cyber hygiene or somebody on your personal computer at home, whether it's a computer at work or a network for a large corporation. The point is to educate folks, get them the training that they need. But really, and that's part of where CISA evolved from out of the legacy NPPD back in 2018.

So really their role is the operational lead for federal cybersecurity to provide that training, to provide some vulnerability assessments to corporations specific to the infrastructure, critical infrastructure in US, all 16 sectors, they're available to assess, provide vulnerability assessments in that. So they can have that one central agency that can be the quarterback spearhead some of that, but obviously they're not the law enforcement arm.

So the Secret Service, the FBI, whoever that may be, will work hand in hand with CISA when there is an incident. Hopefully they have an incident response plan in place, but hopefully law enforcement is part of that plan, and they practice that and keep those close communications with law enforcement. So when there is an incident the first time they pick up the phone and call, it's not a stranger. It's somebody that's either with one of our cyber fraud task force or one of our task force members out in the communities.

Adam Mazmanian:

Now, in that sort of cooperation and partnering, I wanted to ask, because it seems like you hear all the time there's a police department or local hospitals a victim of a ransomware incident. But in addition to sort of pure play cyber crimes, there's also a digital component to a lot of what we would think of as traditional crimes. People who are money laundering to disguise or legal profits in drug dealing or smuggling other aspects. What do you do, what specifically does Secret Service and other agencies do to support local law enforcement when they need that capacity to chase down cryptocurrency, chase down the financial proceeds? What's basically just sort of a traditional criminal activity?

William Smarr:

Great question. Again, what the Secret Service does, and this has been our task force model, and this started back in 2008, was we partnered with the state of Alabama, the prosecutor's office there in Alabama, and the city of Hoover, Alabama, and created the National Computer Forensics Institute. What this is, it's a state-of-the-art facility funded by the federal government, specifically through the Secret Service to train state, local, tribal, territorial officers, judges, and prosecutors to combat cyber crime.

So with that funding, I think we started low, maybe 4 million or so, trained a couple hundred folks back in 2008. That mission, and that has since grown. I think we've trained over 25,000 state and local officers to this point. The budget is probably tenfold of what it started, and we're averaging about 4,000 to 4,500 officers per year being trained. When we say training, we provide the training. We also provide the equipment that they can take back to their communities to work those cases.

When they do get a call at a local PD versus the Secret Service, they most more than likely have somebody in their house that can work that type of crime. It's very specific, electronic exam, forensic examiners and network intrusion, forensic analysts, that type of thing that can get in the weeds and actually do the technical piece of those investigations.

Adam Mazmanian:

That sort of leads into another question, which is of interest to, I think, to at least FCW readers is on the acquisition front. This is a very sort of complicated area to delve into. Are you also giving advice on acquisitions piece so that when they go out to make their own kind of cybersecurity toolkit buys that they're not just starting from scratch?

William Smarr:

Well, I think with what the Secret Service does, obviously we don't point anyone in any certain direction on what they do, but we try to set up some best practices as far as cyber instant response plan, what they have in place there, what tools they're looking through, make sure they're doing their due diligence for the service level agreements, that type of thing. Hopefully the bigger corporations are already doing that. Some of the smaller organizations may not have that expertise, I would say, to do that. But along with the Secret Service, other agencies to include CISA, provide that is good go buys and there's checklists of "These are the things you need to look out for when you are standing up your security systems."

Adam Mazmanian:

Then I think you touched on this in another answer, but just another piece is the sort of cyber hygiene of these local, tribal, state law enforcement organizations themselves. They're probably not in the same place as federal agencies. Are you helping them to keep their own house in order on the cyber side?

William Smarr:

Well, again, when it comes to cybersecurity and the investigative piece and cybersecurity, the IT piece, couple, two different areas, but hopefully one benefits the other. So if they have their folks that are trained in-house to look for bad guys out in other systems and other networks, hopefully they're leveraging that expertise in their own shop to make sure that they're protecting themselves as well.

Adam Mazmanian:

Then with the dawn of cryptocurrency, it was sort of build as, "This is a super secret, anonymous method of moving money. It's completely out of the scope of law enforcement. It's end-to-end encrypted." But it turns out, no, that's not the case. There are companies that are building up capacity and trying to trace and identify and help prosecute people who use cryptocurrency in money laundering, ransomware, and other crimes. Can you talk a little bit about how that capacity developed and what Secret Service does to leverage that?

William Smarr:

Sure. Absolutely. You're exactly right. When Crypto first popped up many years ago, it was a new untraceable internet money, what some people thought. But again, like I spoke earlier, at the end of the day, there's somebody behind a keyboard; there's somebody that's making that transaction occur. With cryptocurrencies, and I'll speak specifically to the illicit money laundering folks groups, many of which are the transnational organized groups. They still leverage the US banking system.

They rely on that US banking system, both for the on-ramp and off-ramp to get that money from a fiat currency to a digital currency and then into a cryptocurrency onto the blockchain. So it's not untraceable. It's difficult to trace, but it's not impossible, and that's why we have the trainings at the NCFI for our state and local partners. The Secret Service does their own training for the crypto tracing, working with private sector partners to help develop those tools. That's going to help find out where that money enters, where it exits, and really to bring that attribution back to folks that are defrauding these victims in the US.

Adam Mazmanian:

Bill, you were in the news a little bit last fall. You co-lead the Operation Crypto Runner investigation to disrupt crypto-based money laundering networks. Can you talk a little bit about that case and how some

of the things that have been part of our Q&A so far played into building that case and what you learned from it? Maybe specifically what it says, how it speaks to cross agency partnerships, collaboration in these kinds of investigations?

William Smarr:

Yeah, absolutely. Operation Crypto Runner, which I think was the first thing in news probably was last fall, but it again, undercover cryptocurrency, money laundering investigations, where really we targeted those over-the-counter exchanges. These folks that were not following the typical rules for the money laundering BSA Bank Secrecy Act guidelines, Know Your Customer, they weren't following these rules. So again, that's a violation and that's a money laundering investigation that we delved into. I think to date, we've arrested over 20 individuals across the US and abroad. I think the average right now is probably stopping about 300 million in illegal illicit money laundering investigations per year. So this investigation's a couple years in the making, and it continues to show those dividends.

But I think just the training that I've talked about, the new technology, making sure that the investigators today that used to investigate the traditional bank fraud, money laundering charges, understand how to do that very same investigation using old-fashioned police work. But with the new technologies on how to analyze and trace money through the blockchain, see where it comes on, see where it comes off, identify when you're doing search warrants, what a wallet address looks like, what seed words look like. Many things, maybe 5, 10 years ago, a detective investigator may have done a search warrant and really not knowing where that information or what it was when they saw it.

So education is a big piece of it. Training that individual to take that information, handle it for the evidentiary value it has, and then be able to present that to a prosecutor's office or a court to have somebody held responsible for. Again, the victims in every one of these cases typically are targeting elderly US citizens, whether it be a romance scam, BEC, business email compromise, telemarketing scam. Most of all, that money gets funneled back into a crypto wallet somewhere and then resides in control of some of these transnational organist criminal groups.

Adam Mazmanian:

You sort of touched on this, there's really a chain of people who have to have some familiarity with how these investigations work in order to get from investigation to successful prosecution. How do you get attorneys, and especially judges, they're going to have to get up to speed on these kinds of issues? I mean, that must be a bit of a lift to get judges to become familiar with the technology and just to believe that this investigative process is actually doing what it says it does.

William Smarr:

Yeah, absolutely. It's a great point. I think our federal partners, we have great partners at the US Attorney's Office in Eastern District of Texas that we work Crypto Runner through. But in addition to that, our state and local, not only prosecutors but judges through the NCFI, the National Computer Forensics Institute, we can also nominate judges and prosecutors to go up and take classes on, "Hey, this is what the evidentiary process is going to look like from the investigator's point of view." Actually, we have mock classrooms at NCFI, and they can actually hold mock trials there introducing the evidence, showing the chain of custody for that electronic evidence and how to hold that person accountable for their actions.

Adam Mazmanian:

You had another law enforcement partner in the Crypto Runner, correct? I was it the USPSOIG was involved and others, can you talk a little bit about how that came together?

William Smarr:

It does, absolutely. Part of this case, just based on the scope and the scale of the case, it ended up being an OCDETF case, which is the Office of Organized Crime Drug Enforcement Task Force. Although there wasn't a drug nexus, there was always going to be drug activity based on illegal activity that they launder those funds. That becomes a financial crime once they start laundering those funds. But definitely we partner with the US Postal Inspection Service and then also with the Diplomatic Security Service to have that overseas presence with some of those folks were overseas using passport fraud and different things to, again, they leverage the US banking system. So some of the money mules, as they're called, sometimes unwitting, sometimes knowing what they're doing, setting up bank accounts in the US illegally with fictitious information.

Some of those were fake passports that the DSS was able to help work that angle, and then the US Postal Inspection Service as well, great partners having their purview over the mail system. Many times the fiat currency that has exchanges hands as mailed through the US Postal Service, and then into a money mule's hands, who then takes that and puts that into a bank account, typically to convert it, and move it into a cryptocurrency. So great partners, the success the Secret Service has had is very much relied on our partnerships from protection to investigations is no different here with the Postal Inspection Service than our partners at DSS.

Adam Mazmanian:

Yeah. It sounds like you need to really have a sense of who has their eyes on what, whether it's overseas or the postal service investigators having access and authority to probe the mails. What are some other, just maybe historically, some other agencies that you've had partnered with as a part of this Crypto investigations?

William Smarr:

Like I said, we talked about it a couple times. This whole of government or whole society approach. There's not one agency, whether it's a Secret Service or any other agency, that's going to be able to combat this cyber crime way that we're seeing the continually, right? Anytime there's something new that comes out, a cyber criminal organized group's going to leverage that to make some illegal funds. But we've partnered with all other agencies, FBI. Secret Service Partners with HSI. You name it, we partner with them. Any crime that comes across, there's always a cyber nexus to that at some point. And through our cyber fraud task forces, we have the ability to, whether it's our individual investigation or investigations, to support others. We partner with all of our federal partners. So there's nobody left out. If I do leave somebody out, I'm sure we work with them as well.

Adam Mazmanian:

Then another question is maybe in 2015, 2016, people were looking at crypto as, "Is this going to catch on? Is this going to be a thing?" What's the next thing that you're looking at? What's sort of beyond the horizon for you in terms of cyber or computer-enabled crimes that you're starting the seed bubble up?

William Smarr:

Yeah. Well, I think again, if the criminal investigator, the federal agent, they're mandated, their charge is to arrest folks that violate federal law. For us, it's anything that has to do with money and violating those criminal acts that are disrupting the financial infrastructure. So I think you hear it in the news every day with artificial intelligence, how's that going to play out at some point, right? The goal is to hold somebody accountable for victimizing someone else.

Well, as you move forward and criminal groups start leveraging AI, that may throw another wrench into it. Again, it's on, it's online, it's not going away. I think we're always going to be able to trace somebody down. You may have to take a few more steps, but I think there's no doubt that the expertise in the grit that the US federal law enforcement and our local state partners have, there's not going to be anybody that we're not going to be able to find. It may take just a hair longer.

Adam Mazmanian:

All right. Well, Bill, we're right at time. I want to thank you again for sharing your expertise with us. With that, I'm going to turn things over to my colleague, Chris Teale, for our next session for FCW. I'm Adam Mazmanian.