Kevin Minor: 0:04
Episode six the NASPO Pulse. This is the podcast where we are monitoring issues in state procurement. We've got our finger on the pulse. I'm your host, kevin Miner, and man, do we have a show for you today? I have the pleasure of being joined by my friend and colleague, olivia Hook-Fry.

Olivia Hook Frey: 0:24
Hey, kevin, thanks for having me Happy to be here today.

Kevin Minor: 0:26
Yes, it's really awesome to have a colleague co-hosting with me. Olivia is the NASPO Director for Member Engagement and Strategic Partnerships and we are co-interviewing Deputy Assistant Director John Jimenez of the FBI.

Olivia Hook Frey: 0:43
Thanks, Kevin. I'm really excited about this episode. During the coronavirus pandemic, chief procurement officials have been leading the charge in finding PPE and other critical items for their states. Unfortunately, due to the high demand and quick turnaround, fraud is at an all-time high. There are many who seek to take advantage of those in need for personal financial gain. A few weeks ago, NASPO was contacted by the FBI. Their team is at the forefront of dealing with fraudulent suppliers and they want to get word out about how to avoid these bad actors. The FBI team has shared with us a press release that includes risk mitigation factors as well as indicators of fraudulent PPE to look out for.

Kevin Minor: 1:18
Thanks for that context, Olivia. But before we talk to Deputy Director Jimenez, here's a message from our 2020 NASPO President, George Shutter.

George Schutter: 1:28
Thanks, kevin. This is George Shutter. I'm the president of the National Association of State Procurement Officials and also the chief procurement officer for the District of Columbia. You know COVID has really required public procurement professionals to adjust from our typical contracting mechanisms Urgent needs, fluent requirements, emergency procurement procedures to meet to really meet our first responders' needs to keep them out of harm's way. Needs to keep them out of harm's way.

George Schutter: 2:09
Cpos procurement professionals, contracting officers are really in a unique position to understand the details of the business transaction and to be a partner to prevent fraud and to have insight where there is, where there are issues In the district, like I know in other state jurisdictions.

George Schutter: 2:28
I've got a great relationship with our inspector general and with our attorney general and those that are on the front end of fighting fraud and do partner with them, and I know from our colleagues around the states that they do the same.

George Schutter: 2:48
This has maybe a silver lining out of COVID, but this has given an opportunity even to further the relationship that we've got throughout the states a bit more cohesively nationally through NASPO and with our colleagues in the FBI, having both an outlet that states are able to share challenging procurements that they have, but also for our states and the district and jurisdictions public procurement professionals to share market research that they have found, to be able to share DeBard lists, for example and to learn contemporaneously about challenges that they're having with procurements From the get-go in the district. With PPE, for example, just the best practice was to use

FaceTime and to actually see product before we would close a deal. But great opportunity here to share some best practices, to illustrate the partnership that NASPO and the FBI have had and to really think also about best practices here in the future that we can continue to improve our mechanisms for public procurement and doing the right thing for the public. Good Thanks, kevin.

Kevin Minor: 4:20
Absolutely, george. Thank you, and now, without further ado, our interview with Deputy Assistant Director John Jimenez. John, thank you so much for joining us on the Pulse today. How are you?

John Jimenez: 4:34
I'm great, Kevin. Thank you for having me.

Kevin Minor: 4:38
Absolutely. We're really excited to be talking to you. This is a very unique episode and I want to dive right in. John, you work for the FBI, you're the Deputy Assistant Director and that is a fascinating career path. Can you give us just a little bit of your background and how you came into your role with the FBI?

John Jimenez: 5:01
Sure, I appreciate you uh, I appreciate the fact that you think it's a fascinating career at its moments from time to time. Uh, I'm in my 24th year now, wow, uh, which makes me a? Uh, a veteran. Um, and I started out in Chicago field office. That was my. That was my first assignment, um, I had uh a uh training agent there, an old training agent that um, very early on in my career, told me that if the FBI wanted me to have a wife, they'd assign me one. Fortunately for me, they did. Uh, my wife was also an FBI agent.

Kevin Minor: 5:45
Oh wow, they actually did.

John Jimenez: 5:48
And yeah, and so yeah, we joke all the time the FBI did assign me a wife. We then went to a Springfield division, fairview Heights Resident Agency, which is the Metro East side of St Louis, missouri. We were there for eight years, then went to Miami where I took a supervisor role, and that was interesting and still benefits me currently, as I was a supervisor of the Mortgage Fraud Squad, and that was 2008, during the housing market. And then the last economic stimulus recovery act was in 2008. And so a lot of the same frauds and scams and schemes that we're going to see with this newest stimulus package that we experienced back then. So I'm fortunate to have had that experience. And then I went to Counterterrorism Division, the Washington field office, and now in the Criminal Investigative Division.

Kevin Minor: 6:57
The world has been keeping you busy.

John Jimenez: 7:00
Yes, we've definitely been busy as of late.

Olivia Hook Frey: 7:13
John, your team got in contact with us several weeks back. Yes, we've been definitely been busy as of late. How our CPOs and their staff are working in the front lines of acquiring PPE and other important items for their states. I think it's really interesting for our listeners and, if you feel comfortable sharing this, John, can you tell us a little bit about your unique connection to chief procurement officers or to our world?

John Jimenez: 7:38

Sure it's, I mean, one of the reasons why it's so important for the FBI to have really strong relationships with our private industry partners, especially in times like these when we want to understand what type of crimes are occurring. Happened to be fortunate that my uncle not only my uncle, but we're very close friends speak on a regular basis as a chief procurement officer, and early on in the crisis situation we're in, I was having regular conversations with them and he was expressing just how frustrating it is in his position, how challenging it is for state procurement officers that are under a tremendous amount of pressure to, as quick as possible, purchase PPE.

John Jimenez: 8:40
That's incredibly hard to come by anyway, that's incredibly hard to come by anyway, and in that conversation you know we just started touching on some. He was telling me about some of the questionable emails that he was receiving offering PPE. And you know, in that conversation we talked about how the FBI could help across the entire country get a message out to as many procurement officers as possible and help them be smart about the way they go about purchasing PPE. And that's when he informed me of NASPO and we were able to get in touch with the guys and it's just been great ever since and it's an outstanding opportunity for us to be able to communicate to all the state procurement officers at the same time.

Kevin Minor: 9:37
So to that point, the FBI provided an industry alert that warned government and healthcare industry buyers of fraudulent trends in PPE specifically, and the alert says that multiple incidences in which the state government agencies attempting to procure such equipment wire transferred funds to fraudulent suppliers in advance of receiving the items. So, john, can you elaborate on any of these incidents and perhaps maybe a specific scheme that's already been charged Sure?

John Jimenez: 10:15
It's a great question. In the wake of COVID-19, states have had to essentially compete with one another to obtain life-saving PPE for their medical professionals and essential workers. We've seen numerous instances of state procurement officials attempting to purchase large quantities of PPE only to find that the money was actually sent to fraudsters, often located overseas, posing as legitimate businessmen, and a million dollars have been lost. Unfortunately, we can't comment on any ongoing investigations which a lot of the advanced fee schemes we're seeing are currently ongoing. A lot of the advanced fee schemes we're seeing are currently ongoing. But we have recently charged a PP fraud case that you might find interesting, and in that case the case was out of New York.

John Jimenez: 11:11
New York field office did a tremendous job of working with our Los Angeles field office field office and it was a situation where a California couple were arrested in an alleged PPE selling scam.

John Jimenez: 11:29
Basically, the fraud involves two purported personal protection equipment dealers and their efforts to scam investors out of millions of dollars. The scheme basically was that they cast themselves as sellers of scarce protective equipment and then tried to entice investors with photographs of boxes of masks they would, you know, offer to. They would claim that they had contracts and agreements to sell millions of masks and that they didn't even actually own the investors. One particular investor who helped tip us off to the case was asked to wire $4 million. He became suspicious and informed us, uh, and then he agreed to follow the fraudster's instructions, uh, to come and inspect the merchandise. Um, and in essence what they did was they had a box of real merchandise and then a whole lot of pretend boxes of merchandise. Wow, and then, fortunately, we were able to figure out that the the product that they did have wasn't even real, certified PPE. So we were able to arrest the two and charge them.

Kevin Minor: 13:02
Wow. So not only was the equipment that they actually physically had was counterfeit, but then they just had a bunch of virtually empty boxes behind that, Right right and so counterfeit is a funny term.

John Jimenez: 13:20
Right, right, right and so counterfeit is a funny term. Right, because one of the things that we're seeing we've seen it you may see in the press about the Department of Homeland Security's I think it's called Stolen Promises is their operation name and you know in the press they reported as counterfeit items that are being seized. What's really happening oftentimes is that it's actually prohibited items that are being stopped at the border by border patrol. So fortunately, we're not seeing a lot of actual counterfeit, not seen a lot of actual counterfeit. There is some out there, but we're not seeing a lot of counterfeit items as much as we are items that are being purported to be something that's certified and then it's really not so, and that's one of the things that we are hopefully able to warn procurement officers about.

Olivia Hook Frey: 14:24
That brings up a great point. You know, I know the N95 masks were kind of the top item that our states were looking for over the last few weeks and months now, and I know a couple of states with the lack of N95 masks available and the shortage that we're experiencing for a while they were looking at some other masks that maybe were similar. So I think you know, with the specifications changing slightly or if they're similar enough, I know there's a lot of nuances there, but I think something like that would make it even more difficult to make sure that you're getting you know legitimate, yeah, yeah absolutely um, and and there is, there's even, as I understand it, uh.

John Jimenez: 15:09
so when the kn95 masks out of uh were approved, the certified out of china, it was only for a particular serial number, a particular model, and unfortunately, what we're finding is a lot of that is not the particularly approved FDA approved model.

Kevin Minor: 15:34
That's a really interesting distinction that I didn't think about at all. There's not only counterfeit merchandise, but there's also merchandise that just didn't think about at all. There's not only counterfeit merchandise, but there's also merchandise that just isn't approved and either way, the buyer is not getting what the contract specified. Right, that's correct.

John Jimenez: 15:55
That's correct and I think there's an interesting dynamic too, because I think, from what I've seen, some of the state procurement officers are where typically their experience is in setting up contracts and ordering material, so the pressure to order this stuff quickly and in volume, and then they're being asked to, in essence, kind of be the verifiers of what they're getting as well, which is maybe not something that they're normally used to doing. So anything we can do to get them information about how to go about verifying what they're purchasing is correct. We'd love to look to help to do that. 3m has been a great partner to us and in the liaison information report you'll see that recommendations from 3M in terms of when purchasing the 3M products, kind of what to look for and how to go about doing that safely.

Kevin Minor: 17:06
So let's talk risk mitigation factors. The alert also says that in the current environment, certain medical equipment demand far outweighs supply and that it is quote ripe for fraudulent actors.

John Jimenez: 17:25
Yeah. So the interesting thing about fraud and working white collar for the FBI is fortunately, at the end of the day, there's only a handful of schemes that the fraudsters can use. That the fraudsters can use, but then the way that they dress it up and market it and sell it changed to suit the particular situation. And that's what we're seeing now is that they recognize being incredibly resourceful which is oftentimes what makes them successful fraudsters is recognizing those opportunities to exploit and they've recognized that the state procurement officers are under a tremendous amount of pressure there is, you know, we've had conversations with 3M that it is where they are in

essence, where they are in essence saying it is next to impossible for states to be able to purchase 3M material from an authorized distributor, because the authorized distributors are dealing directly with the hospitals and various healthcare and from FEMA as well healthcare and from FEMA as well.

John Jimenez: 18:40
Then FEMA's redistributing it to the places where, where they, where they want it to go to. So knowing that ahead of time makes it incredibly frustrating for the state procurement officers who have to try to purchase the product and and it's very difficult to find a safe and legitimate way to purchase it. And so fraudsters know that and they're ready to fill a role, or at least pretend to fill a role that's needed in order to try to steal people's money. Steal people's money.

Kevin Minor: 19:20
Well, and so it sounds like fraudsters are being. They have to be creative in a in a sense, and does that? You know? How have you seen fraudsters? That's an interesting term.

John Jimenez: 19:36
How have you seen them to be creative? Yeah, yeah, and you know, I mean I'm fairly certain that people listening will understand what a fraudster is. It's just somebody who commits fraud and potentially deceiving victims, uh, for the purpose of financial gain. And with regards I mean what, what you usually end up seeing is they will evolve as quickly as we can warn the public about the particular window dressing that they're putting on a scheme. They will then use that as intelligence and alter their scheme. So, for example, I think in one of the first public service announcements we put out about advanced fee schemes, we talked about the potential to use escrow, an escrow account, as a possible way to avoid being scanned, and then what we saw pretty quickly was then the fraudsters were utilizing that information and incorporating that in their scheme as window dressing, their scheme, setting up bogus escrow accounts in order to make the purchaser feel more comfortable working with them.

Olivia Hook Frey: 21:05
It's tough because your team is working so diligently to get the word out to the public, to as many people as you can who are doing the purchasing, but, like you said, the fraudsters are right on your tail. So it's difficult because the people who need to see the message it's public, so these fraudulent people are still are seeing it as well.

John Jimenez: 21:18
Mm-hmm. Yeah, absolutely, that's the dilemma that we deal with, and it's just as quick as we see it. We just need to try to continue to warn the public.

Olivia Hook Frey: 21:31
So, talking about mitigating risk, of course our chief procurement officers, they're stewards of taxpayer dollars. They want to mitigate risk, especially in a high pressure situation like this. One of the ways that some of our states are trying to avoid these fraudsters we've heard the District of Columbia has used FaceTime to work with suppliers to actually visualize some of this equipment. Are there any other examples that you've heard or that your team can offer to avoid this?

John Jimenez: 22:05
Yeah, that's interesting because that's you know, we were just talking about the fraudsters adapting the way that they try to sell their scheme. In addition to them adapting to utilizing escrow accounts or fake escrow accounts, we've also seen them now adapt to talk about that. They are working directly with 3m, that they've somehow in some fashion come upon a tremendously large number of PPE and they will only deal in very large amounts. Obviously, that's to increase the amount of money that they can steal and then offering to have the merchandise inspected so you can travel somewhere and inspect it, and the assumption is, if it's fraud is that it'll be similar to the case that I talked about, where they will have maybe a very small amount and but make it look like they have more

than more actual product than what they really have.

John Jimenez: 23:15
So some of the I think some of the red flags you know is that if any of your procurement officers receive an unsolicited email or phone call from a company which they haven't previously done business with, I think it's important that your network of procurement officers work to communicate across and hopefully through you and as they identify reputable vendors, legitimate vendors, vendors that they've done work with before and vendors that they are actually receiving product from, and hopefully you can help refine your list of approved vendors. If they receive an email from a business with which they previously conducted business with, but are all of a sudden asking for a change in the payment process, right, that could be also a red flag. If the company advertises that they have massive amounts of PPE, which you just talked about, readily available, that's automatically something that the procurement officer should be suspicious of, because it is just incredibly hard to obtain right now.

Olivia Hook Frey: 24:38
Right.

John Jimenez: 24:40
Especially if they're claiming that they're working with 3M in some form or fashion, and 3M will be the first to tell you that they don't deal with escrow accounts. And so in the liaison intel report there's additional red flags that 3M provided. So I would recommend that your listeners take a look at that.

Olivia Hook Frey: 25:06
So what we've tried to do is we've pivoted, as many people have over the last several weeks, to do some research into some of these suppliers. So some of the categories that we're looking into and I kind of want to run these past you and see what you think if there are any other categories you can think of in researching these supplier emails or calls. We're looking at. When they were founded are they a company that's been around for a while? Did they get incorporated last week? Where they're located? Contact information, number of employees other contracts sales, business registrations.

Olivia Hook Frey: 25:45
You know if we've worked with them in the past and via our cooperative purchasing arm, all these different categories. Are there any other categories or any other things you think that we should look for Now? You mentioned the website name, the domain.

John Jimenez: 25:59
You know you've said a lot of the important things that they can do to protect themselves, and I think you know the one other thing I will I will say is it's challenging, right, because what I've learned is that oftentimes there can be a vendor that maybe a procurement officer has dealt with in the past, and that vendor then is lured by the offer of tremendous amount of PPE, you know, direct from 3M, and so they're passing it on and they're doing what vendors do, and they're passing that information on, but the procurement officer is really believing that that it's it's accurate, and so that makes your job that much more difficult, and so I would just say that there may be, there may be some due diligence necessary, not only only with who the vendor that the contract is with, but also digging a little deeper and past that to find out more about the supplier.

Olivia Hook Frey: 27:00
Yeah, that's a great point. You can't be too careful.

Kevin Minor: 27:03
Right and, to that point, what are the broader efforts that you guys are doing right now to educate the public and what are some of those lessons learned?

John Jimenez: 27:16
Yeah, so I mean, like I mentioned, the FBI has released several public service announcements and you know you can find them on the on the FBIgov website Industry alerts, you know, such as the one that we've talked about, to inform the public of the COVID-19 scams that we're seeing and kind of what they can do to protect themselves. We have and will continue to engage with the news media to get the message out, and anything like this fantastic opportunity to be with you on the podcast and opportunities anything opportunities that we can to get the message out is what we're doing, and we're working closely with our partners in private industry, like NASPO and 3M, state and local governments and other law enforcement agencies to share information as proactively as possible, which is precisely why we believe it is so important to speak to you and your colleagues today.

Olivia Hook Frey: 28:18
Yeah, we're so glad to have you. We've been quick to share some of the resources that you and your team have shared with us, with our members. But I think it's different to hear it from you who's working in the front lines to stop these fraudulent actors. It's different hearing it from the horse's working in the front lines to stop these fraudulent actors. It's different hearing it from the horse's mouth.

Kevin Minor: 28:37
Yeah, when we just appreciate, you know, being able to get your message out and the help that you guys are. You know the efforts that you guys are doing right now to actually catch these bad actors. You know there's nothing really worse than you know these bad actors. You know there's nothing really worse than you know someone taking advantage of the fear and alarmism in today's current escape, the way things currently are. We appreciate the opportunity to get the message out. Yeah, absolutely, and listen.

John Jimenez: 29:05
If, if, uh, if people don't report it, if they don't report what they're seeing, if we don't know about it, then we can't help stop it.

Kevin Minor: 29:14
Well, that actually brings me to my next question. If CPOs, procurement staff, if they do see that suspicious behavior, how do they go about reporting it, and why is reporting so important?

John Jimenez: 29:29
Sure. So we can't stress enough that what we would recommend is that they report the incident to wwwic3.gov and not an or but an and contact your local FBI field office and both do both things. Yeah, definitely do both. So IC3 is FBI ran clearinghouse for reporting fraud, internet fraud and various types of fraud, and it gives us a chance to assess the information. But also it gives us a chance to assess the information with perspective across the entire country.

John Jimenez: 30:18
What I mean by that is why it's so important is, if a procurement officer is defrauded on a very small order let's say $50,000, it's a lot of money, but in terms of federal crime and the whole scheme of law out there, that particular $50,000 loss may fall in priority.

John Jimenez: 30:48
Or state authorities, maybe the state attorney general, because we just wouldn't have time to look at every single small dollar fraud. There's just too much of it. Right, we don't have the resources, but if that same fraudster now defrauds 10 states of $50,000, we have a picture then of what's happening nationally and all of a sudden we can identify that there's multiple victims and a much higher dollar loss and then, uh, direct a particular field office to to look into it. So, uh, so we can't stress that enough. It's worth the time. If a procurement officer has already transferred funds and believes it may have been a fraudulent transaction, I would recommend that they contact the

financial institution immediately to make them aware so definitely you know, because, like you said, that fifty thousand dollars can turn into several million dollars pretty quick.

Kevin Minor: 32:02
If it's not tracked, if there's no data, if, if you're not able to identify a pattern correct, correct and there's.

John Jimenez: 32:11
You can't. You know, I would, I would tell your listeners that you can't. There's no such thing as over-reporting, and so I would highly recommend that they take advantage of both IC3 and the local FBI office and, you know, potentially the state attorney general right, the local prosecutor's office. I mean, I would never say that they shouldn't try to report it to all possible venues to get some sort of recourse as quick as possible.

Kevin Minor: 32:51
You know, John, we really want to focus on getting your message out. Is there anything else that we didn't highlight, that that perhaps we should have talked about?

John Jimenez: 33:03
No, I mean I would just say when purchasing PPE or conducting large financial transactions in the course of business, just as much as you can slow down and do your due diligence, contact the FBI and your financial institution quickly If you even suspect that something's not right it you know it.

John Jimenez: 33:25
It may cost you a day in terms of being able to get the material, but it may end up saving, saving you millions, millions. I think it's also important to stress that, in terms of reporting, not to be embarrassed I mean, fraudsters are skilled at their craft, right, they're very good at what they do, otherwise it wouldn't exist, it wouldn't be worth it for them. And so, reporting to IC3 and your local FBI office, it may just be the missing puzzle piece to a larger fraudulent enterprise. So when victims report even relatively small losses, right, we can uncover large schemes. And when we get to aggregate the data, allowing us to shut down their operations, prevent further victimization and potentially, you know, even recover some of the funds. So that's our goal.

Olivia Hook Frey: 34:22
John, on a personal note, I have to ask, with your long career and seeing the things that you've seen and working on the projects that you've worked on, how much faith in humanity do you have left after seeing all this? I'm sure that kind of skews your, your view of humanity in a way.

John Jimenez: 34:40
Yeah it, it definitely can. It's it's easy to get jaded in the law enforcement profession. Yeah Right, it's. It's kind of what we in the law enforcement community signed up to do is to kind of stare that evil in the face and on a daily basis and try to combat it. Sometimes it feels really rewarding, like we're winning, and other days it doesn't necessarily feel like like we're winning. So, uh, I think you know, uh, early on in in the mid 90s, uh, when I was working narcotics, um, and it was very easy to be jaded and feel like what you were doing was never going to make a difference, and I think I just finally realized, realized that it's better to do something than nothing. So that's kind of the way I look at it, right.

Olivia Hook Frey: 35:39
And two plus decades later, you're still doing it. So I'll give you credit Still going strong, still going strong.

Kevin Minor: 35:47
John Jimenez, deputy Assistant Director, my guest today. John, thank you so much.

John Jimenez: 35:54
Thanks, kevin. I really appreciate you giving me this opportunity to work with you, and I appreciate our partnership.

Kevin Minor: 36:02
Absolutely, and maybe we'll have you back on the pod once this is all over and we can talk about something a little more uplifting.

John Jimenez: 36:07
I'd appreciate that.

Kevin Minor: 36:10
Better to do something than nothing. I think Special Agent Jimenez is right. I think that that's something we really need to stop and appreciate. During this time, we've had a lot of conversations about COVID-19, I know, but it's because it's so relevant. It's literally shaping the world that we live in. It's good to take a step back and reflect as to not be so jaded. Like he said, you take care of yourselves out there.

Kevin Minor: 36:39
I'd like to thank my co-host, olivia Hook Frye. If you have any questions about NASPO COVID-19 response, you can check out naspoorg slash COVID-19 dash resources or email membership at naspoorg. We have a lot of great resources that Olivia is coordinating. Also, a shout out to the 2020 NASPO President, george Shutter. Thanks for taking time to record that message for us. Got comments? We'd love to hear them. Email me. Podcast at naspopoorg. Well, that does it for us on the pulse today. If you haven't already, make sure you subscribe to us on apple podcast, spotify, google or wherever you get them listeners. You do not want to be the only person who didn't listen to the pulse. Make sure you check out the blog A lot of really great content written by a lot of really great people and make sure you take a minute for yourself. Today. I'm Kevin Miner. Until next time, thank you.